Bitdefender®

ANTIVIRUS PLUS 2016

BENUTZERHANDBUCH

Bitdefender Antivirus Plus 2016
Benutzerhandbuch

Veröffentlicht 09.09.2015

Copyright© 2015 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und die dazugehörige Dokumentation sind urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „ohne Mängelgewähr" gegeben. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokument entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von Bitdefender erstellte Webseiten, die auch nicht von Bitdefender kontrolliert werden, somit übernimmt Bitdefender auch keine Verantwortung in jeglicher Art für den Inhalt dieser Webseiten. Der Besuch der in diesem Dokument aufgelisteten Drittanbieter-Webseiten erfolgt damit auf eigene Gefahr. Bitdefender stellt diese Links der Einfachheit zur Verfügung. Dies bedeutet nicht, dass Bitdefender den Inhalt einer Website Dritter befürwortet oder Verantwortung dafür übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

Bitdefender

Inhaltsverzeichnis

Installation 1

1. Vor der Installation 2

2. Systemanforderungen 3
   2.1. Mindestsystemanforderungen 3
   2.2. Empfohlene Systemanforderungen 3
   2.3. Software-Anforderungen 4

3. Installieren Ihres Bitdefender-Produkts 5
   3.1. Installation über Bitdefender Central 5
   3.2. Installation vom Installationsdatenträger 8

Erste Schritte 14

4. Grundlagen 15
   4.1. Das Bitdefender-Fenster öffnen 16
   4.2. Probleme beheben 16
      4.2.1. "Alle Probleme beheben"-Assistent 17
      4.2.2. Konfigurieren von Statusbenachrichtigungen 18
   4.3. Ereignisanzeige 18
   4.4. Auto-Pilot 20
   4.5. Profile und Akkubetrieb 21
      4.5.1. Profile 21
      4.5.2. Akkubetrieb 22
   4.6. Passwortschutz für Bitdefender-Einstellungen 24
   4.7. Anonyme Nutzungsberichte 25
   4.8. Sonderangebote und Produktbenachrichtigungen 25

5. Bitdefender-Benutzeroberfläche 27
   5.1. Task-Leisten-Symbol 27
   5.2. Hauptfenster 29
      5.2.1. Obere Symbolleiste 30
      5.2.2. Schaltflächen 30
   5.3. Die Bitdefender-Module 31
      5.3.1. **Schutz** 31
      5.3.2. **Privatsphäre** 32
      5.3.3. **Extras** 33
   5.4. Sicherheits-Widget 34
      5.4.1. Dateien und Verzeichnis scannen 35
      5.4.2. Das Sicherheits-Widget ausblenden/anzeigen 36
   5.5. Sicherheitsbericht 36
      5.5.1. Aufrufen des Sicherheitsberichts 38
      5.5.2. Aktivieren oder Deaktivieren der Benachrichtigungen zum Sicherheitsbericht 39

6. Bitdefender Central 40
   6.1. Aufrufen Ihres Bitdefender Central-Benutzerkontos. 40

6.2. Meine Abonnements . . . 41
6.2.1. Verfügbare Abonnements anzeigen . . . 41
6.2.2. Ein neues Gerät hinzufügen . . . 41
6.2.3. Abonnement verlängern . . . 42
6.2.4. Abonnement aktivieren . . . 42
6.3. Meine Geräte . . . 43

7. Bitdefender auf dem neuesten Stand halten . . . 46
7.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist . . . 47
7.2. Durchführung eines Updates . . . 47
7.3. Aktivieren / Deaktivieren der automatischen Updates . . . 48
7.4. Update-Einstellungen anpassen . . . 48

Gewusst wie . . . 51

8. Installation . . . 52
8.1. Wie installiere ich Bitdefender auf einem zweiten Computer? . . . 52
8.2. Wann sollte ich Bitdefender neu installieren? . . . 52
8.3. Wo kann ich mein Bitdefender-Produkt herunterladen? . . . 53
8.4. Wie verfahre ich mit meinem Bitdefender-Abonnement nach einem Windows-Upgrade? . . . 54
8.5. Wie kann ich Bitdefender reparieren? . . . 57

9. Abonnements . . . 58
9.1. Welches Bitdefender-Produkt nutze ich? . . . 58
9.2. Wie kann ich mein Bitdefender-Abonnement mithilfe eines Lizenzschlüssels aktivieren? . . . 58

10. Bitdefender Central . . . 60
10.1. Wie melde ich mit einem anderen Benutzerkonto bei Bitdefender Central an? . . . 60
10.2. Wie setzte ich das Passwort für mein Bitdefender Central-Konto zurück? . . . 60

11. Prüfen mit Bitdefender . . . 62
11.1. Wie kann ich eine Datei oder einen Ordner scannen? . . . 62
11.2. Wie scanne ich mein System? . . . 62
11.3. Wie plane ich einen Scan? . . . 63
11.4. Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen? . . . 63
11.5. Wie kann ich einen Ordner vom Scan ausnehmen? . . . 64
11.6. Wie gehe ich vor, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat? . . . 65
11.7. Wo sehe ich, welche Viren Bitdefender gefunden hat? . . . 66

12. Privatsphärenschutz . . . 68
12.1. Wie sichere ich meine Online-Transaktionen ab? . . . 68
12.2. Wie lösche ich mit Bitdefender eine Datei unwiderruflich? . . . 68

13. Nützliche Informationen . . . 69
13.1. Wie teste ich meine Virenschutzlösung? . . . 69
13.2. Wie kann ich Bitdefender entfernen? . . . 69
13.3. Wie fahre ich den Computer automatisch herunter, nachdem der Scan beendet wurde? . . . 71

13.4. Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung? 72
13.5. Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert? 73
13.6. Wie kann ich in Windows versteckte Objekte anzeigen? 74
13.7. Wie entferne ich andere Sicherheitslösungen? 74
13.8. Wie führe ich einen Neustart im abgesicherten Modus durch? 76

Die Sicherheitselemente im Detail 77

14. Virenschutz 78
14.1. Zugriff-Scans (Echtzeitschutz) 79
14.1.1. Aktivieren / Deaktivieren des Echtzeitschutzes 79
14.1.2. Echtzeitschutz anpassen 80
14.1.3. Einstellungen des Echtzeitschutzes konfigurieren 80
14.1.4. Wiederherstellen der Standardeinstellungen 85
14.2. On-Demand Prüfung 85
14.2.1. Eine Datei oder einen Ordner nach Malware scannen 86
14.2.2. Durchführen von Quick Scans 86
14.2.3. Durchführen von System-Scans 86
14.2.4. Benutzerdefinierte Scans durchführen 87
14.2.5. Viren-Scan-Assistent 91
14.2.6. Scan-Protokolle lesen 94
14.3. Automatischer Scan von Wechselmedien 95
14.3.1. Wie funktioniert es? 95
14.3.2. Verwalten des Scans für Wechselmedien 96
14.4. Konfiguration der Scan-Ausschlüsse 97
14.4.1. Dateien oder Ordner vom Scan ausschließen 97
14.4.2. Dateiendungen vom Scan ausschließen 98
14.4.3. Verwalten von Scan-Ausschlüssen 99
14.5. Verwalten von Dateien in Quarantäne 100
14.6. Active Threat Control 101
14.6.1. Überprüfen erkannter Anwendungen 102
14.6.2. Aktivieren / Deaktivieren von Active Threat Control 102
14.6.3. Anpassen des Active-Threat-Control-Schutzes 102
14.6.4. Verwalten von ausgeschlossenen Prozessen 103

15. Internet-Schutz 105
15.1. Bitdefender-Benachrichtigungen im Browser 106

16. Identitätsschutz 108
16.1. Endgültiges Löschen von Dateien 108

17. Schwachstellen 110
17.1. Scannen des Computers nach Schwachstellen 110
17.2. Automatische Schwachstellenüberwachung 111

18. Ransomware-Schutz 114
18.1. Aktivieren und Deaktivieren des Ransomware-Schutzes 114
18.2. Schützen Sie Ihre persönlichen Dateien vor Ransomware-Angriffen. 115
18.3. Konfiguration vertrauenswürdiger Anwendungen 116
18.4. Konfiguration blockierter Anwendungen 116

18.5. Schutz beim Systemstart ... 117
19. Sichere Online-Transaktionen mit Safepay ... 118
19.1. Bitdefender Safepay™ verwenden ... 119
19.2. Einstellungen verändern ... 120
19.3. Lesezeichen verwalten ... 121
19.4. Hotspot-Sicherheit in ungesicherten Netzwerken ... 122
20. Passwortmanager-Schutz für Ihre Anmeldedaten ... 123
20.1. Konfiguration des Passwortmanagers ... 124
20.2. Aktivieren oder Deaktivieren des Passwortmanager-Schutzes ... 127
20.3. Verwaltung der Passwortmanager-Einstellungen ... 128
21. USB Immunizer ... 132
Systemoptimierung ... 133
22. Profile ... 134
22.1. Arbeitsprofil ... 135
22.2. Filmprofil ... 136
22.3. Spielprofil ... 137
22.4. Echtzeitoptimierung ... 139
Problemlösung ... 140
23. Verbreitete Probleme beheben ... 141
23.1. Mein System scheint langsamer zu sein ... 141
23.2. Der Scan startet nicht ... 143
23.3. Ich kann eine Anwendung nicht mehr ausführen ... 145
23.4. Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert? ... 147
23.5. Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann ... 147
23.6. Mein Computer ist nicht mit dem Internet verbunden. Wie kann ich Bitdefender aktualisieren? ... 148
23.7. Bitdefender-Dienste antworten nicht ... 149
23.8. Das automatische Einfügen funktioniert bei meiner Geldbörse nicht ... 150
23.9. Entfernen von Bitdefender ist fehlgeschlagen ... 151
23.10. Mein System fährt nach der Installation von Bitdefender nicht mehr hoch ... 152
24. Malware von Ihrem System entfernen ... 156
24.1. Bitdefender-Rettungsmodus ... 156
24.2. Wie gehe ich vor, wenn Bitdefender einen Virus auf Ihrem Computer findet? ... 159
24.3. Wie entferne ich einen Virus aus einem Archiv? ... 160
24.4. Wie entferne ich einen Virus aus einem E-Mail-Archiv? ... 161
24.5. Wie gehe ich vor, wenn ich eine Datei für gefährlich halte? ... 163
24.6. Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll? ... 163
24.7. Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll? ... 164

24.8. Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll? 164
24.9. Warum hat Bitdefender ein infizierte Datei automatisch gelöscht? 164

Kontaktieren Sie uns 165

25. Hilfe anfordern 166

26. Online-Ressourcen 169
26.1. Bitdefender-Support-Center 169
26.2. Bitdefender Support-Forum 170
26.3. Das Portal HOTforSecurity 170

27. Kontaktinformation 171
27.1. Kontaktadressen 171
27.2. Lokale Vertriebspartner 171
27.3. Bitdefender-Niederlassungen 171

Glossar 174

INSTALLATION

1. VOR DER INSTALLATION

Bevor Sie Bitdefender Antivirus Plus 2016 installieren, sollten Sie für eine reibungslose Installation sicherstellen, dass folgende Schritte durchgeführt wurden:

- Stellen Sie sicher, dass der Zielcomputer für die Bitdefender-Installation die Systemvoraussetzungen erfüllt. Wenn Ihr Computer nicht die Mindest-Systemanforderungen erfüllt, kann Bitdefender nicht installieren werden. Wird die Systemkonfiguration nachträglich verändert, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen. Eine vollständige Liste der Systemanforderungen finden Sie unter *„Systemanforderungen“ (S. 3)*.
- Melden Sie sich mit einem Administrator-Konto am Computer an.
- Entfernen Sie alle anderen Sicherheitslösungen von Ihrem Computer. Die gleichzeitige Nutzung mehrerer Sicherheitsprogramme kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Windows Defender wird während der Installation deaktiviert.
- Ihr Computer sollte während der Installation mit dem Internet verbunden sein, selbst wenn Sie von CD oder DVD installieren. Falls neuere Versionen der Anwendungsdateien aus dem Installationspaket verfügbar sind, kann Bitdefender diese dann herunterladen und installieren.

2. SYSTEMANFORDERUNGEN

Sie können Bitdefender Antivirus Plus 2016 nur auf Computern mit den folgenden Betriebssystemen installieren.

- Windows 7 mit Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

Stellen Sie vor der Installation sicher, dass Ihr Computer die Mindestsystemanforderungen erfüllt.

Beachten Sie

Für Informationen zu Ihrem Windows-Betriebssystem und Ihrer Hardware gehen Sie folgendermaßen vor:

- Rechtsklicken Sie unter **Windows 7** im Desktop auf **Arbeitsplatz** und wählen Sie **Eigenschaften** aus dem Menü.
- In **Windows 8 und Windows 8.1**, finden Sie auf der Windows-Startseite den Eintrag Computer (z.B. durch die Eingabe von "Computer" auf der Startseite) und rechtsklicken Sie auf das entsprechende Symbol. Wählen Sie im Menü unten Eigenschaften. Im Bereich System finden Sie Informationen zu Ihrem Systemtyp.
- Geben Sie unter **Windows 10** "System" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol. Im Bereich System finden Sie Informationen zu Ihrem Systemtyp.

2.1. Mindestsystemanforderungen

- 1 GB freier Speicherplatz (davon mindestens 800 MB auf dem Systemlaufwerk)
- 1.6-GHz-Prozessor
- 1 GB Arbeitsspeicher (RAM)

2.2. Empfohlene Systemanforderungen

- 2 GB freier Speicherplatz (davon mindestens 800 MB auf dem Systemlaufwerk)
- Intel CORE 2 Duo (2 GHz) oder gleichwertiger Prozessor
- 2 GB Arbeitsspeicher (RAM)

2.3. Software-Anforderungen

Um Bitdefender und alle Funktionen nutzen zu können, muss Ihr Computer die folgenden Software-Anforderungen erfüllen:

- Internet Explorer 10 oder höher
- Mozilla Firefox 14 oder höher
- Google Chrome 20 oder neuer
- Skype 6.3 oder höher
- Yahoo! Messenger 9 oder höher

3. INSTALLIEREN IHRES BITDEFENDER-PRODUKTS

Sie können Bitdefender vom Installationsdatenträger installieren oder den Web-Installer verwenden, der über das Bitdefender Central]-Benutzerkonto heruntergeladen werden kann.

Wenn Sie eine Lizenz für mehr als einen Computer haben, (weil Sie z. B. Bitdefender Antivirus Plus 2016 für 3 PCs gekauft haben), wiederholen Sie den Installationsvorgang und aktivieren Sie Ihr Produkt mit demselben Benutzerkonto auf jedem der Computer. Dabei müssen Sie das Benutzerkonto verwenden, das Ihr aktives Bitdefender-Abonnement enthält.

3.1. Installation über Bitdefender Central

Über das Bitdefender Central-Benutzerkonto können Sie das richtige Installationspaket für das von Ihnen erworbene Abonnement herunterladen. Nach Abschluss des Installationsvorgangs wird Bitdefender Antivirus Plus 2016 aktiviert.

So können Sie Bitdefender Antivirus Plus 2016 über Ihr Bitdefender Central-Benutzerkonto herunterladen:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie im Fenster **Meine Geräte** auf **Bitdefender installieren**.
4. Wählen Sie zunächst **Windows** und danach eine der beiden Optionen aus:
   - Ich möchte Bitdefender **Auf diesem Gerät** installieren.

     Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus und klicken Sie auf **Herunterladen**, um fortzufahren.
   - Ich möchte Bitdefender **Auf einem anderen Gerät** installieren.

     Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.
5. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

Validierung der Installation

Bitdefender wird zuallererst Ihr System überprüfen, um die Installation zu bestätigen.

Wenn Ihr System die Mindestanforderungen zur Installation von Bitdefender nicht erfüllt, werden Sie darüber informiert, welche Bereiche aufgerüstet werden müssen, damit Sie fortfahren können.

Wenn ein inkompatibles Virenschutzprogramm oder eine ältere Version von Bitdefender erkannt wird, werden Sie aufgefordert, diese von Ihrem System zu entfernen. Bitte folgen Sie den Anweisungen, um die Software von Ihrem System zu entfernen und so spätere Probleme zu vermeiden. Unter Umständen müssen Sie Ihren Computer neu starten, um die Entfernung der erkannten Virenschutzprogramme abzuschließen.

Das Installationspaket für Bitdefender Antivirus Plus 2016 wird ständig aktualisiert. Klicken Sie dazu auf **Ja**, wenn Sie dazu aufgefordert werden. Bitdefender lädt dann die Dateien herunter und gewährleistet so, dass Sie die aktuelle Version der Software installieren.

Beachten Sie

Das Herunterladen der Installationsdateien kann eine Weile dauern, besonders bei langsameren Internetverbindungen.

Sobald die Installation validiert ist, startet der Installationsassistent. Folgen Sie den Schritten, um Bitdefender Antivirus Plus 2016 auf Ihrem PC zu installieren.

Schritt 1 - Installation von Bitdefender

Im Bitdefender-Installationsbildschirm können Sie entscheiden, welche Art von Installation Sie wünschen.

Wenn Sie sich nicht um Detaileinstellungen kümmern möchten, klicken Sie einfach auf **Installieren**. Bitdefender wird dann mit den Standardeinstellungen im Standardpfad installiert, und Sie können direkt mit Schritt 3 des Assistenten fortfahren.

Klicken Sie zur Konfiguration der Installationseinstellungen auf **Benutzerdef.**.

In diesem Schritt können Sie zwei zusätzliche Dinge tun:

- Bitte lesen Sie vor der Installation die Endbenutzer-Lizenzvereinbarung. Die Lizenzvereinbarung enthält die Nutzungsbedingungen für Bitdefender Antivirus Plus 2016.

  Sollten Sie diesen Nutzungsbedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsprozess wird abgebrochen uns Sie verlassen den Assistenten.

- Senden von **anonymen Nutzungsberichten** aktivieren. Durch Aktivierung dieser Option, werden Berichte, die Informationen zu Ihrer Nutzung des Produktes enthalten, an Bitdefender Server gesendet. Diese Information ist wichtig für die Verbesserung des Produktes. Bitte beachten Sie, dass diese Berichte weder vertrauliche Daten, wie Ihren Namen und Ihre IP Adresse, enthalten, noch werden diese Daten für kommerzielle Zwecke verwendet.

Schritt 2 - Installation individuell anpassen

Beachten Sie

Dieser Schritt kommt nur dann vor, wenn Sie die benutzerdefinierte Installation gewählt haben.

Die folgenden Optionen sind verfügbar:

Installationspfad

Bitdefender Antivirus Plus 2016 wird standardmäßig im Ordner C:\Programme\Bitdefender\Bitdefender 2016 installiert. Falls Sie ein anderes Installationsverzeichnis wählen möchten, klicken Sie auf **Ändern** und wählen Sie das Verzeichnis, in dem Sie Bitdefender installieren möchten.

Proxy-Einstellungen konfigurieren

Bitdefender Antivirus Plus 2016 benötigt Zugriff auf das Internet, um die Produktregistrierung abzuschließen, Sicherheits- und Produkt-Updates herunterzuladen, In-the-Cloud-Komponenten zu nutzen usw. Wenn Sie eine Proxy-Verbindung anstelle einer direkten Internet-Verbindung nutzen, müssen Sie diese Option auswählen und die Proxy-Einstellungen konfigurieren.

Die Einstellungen können aus dem Standard-Browser importiert oder manuell eingegeben werden.

Klicken Sie auf **Installieren**, um Ihre Einstellungen zu bestätigen und mit der Installation zu beginnen. Wenn Sie sich später umentscheiden, können Sie einfach auf die entsprechende **Standard verwenden**-Schaltfläche klicken.

Schritt 3 - Installation wird durchgeführt

Bitte warten Sie, bis der Installationsvorgang abgeschlossen ist. Sie erhalten detaillierte Informationen über den Fortschritt der Installation.

Kritische Bereiche Ihres Systems werden nach Viren durchsucht, die neuesten Versionen der Anwendungsdateien heruntergeladen und installiert und die Bitdefender-Dienste gestartet. Dieser Schritt kann einige Minuten in Anspruch nehmen.

Schritt 4 - Installation ist abgeschlossen

Ihr Bitdefender-Produkt wurde erfolgreich installiert.

Eine Zusammenfassung der Installation wird angezeigt. Sollte während der Installation aktive Malware erkannt und entfernt werden, könnte ein Neustart des Systems erforderlich werden. Klicken Sie auf **Weiter**.

Schritt 5 - Erste Schritte

Im Fenster "Erste Schritte" können Sie sehen, wie lange Ihr Abonnement noch gültig ist.

In diesem Schritt können Sie zwei zusätzliche Dinge tun:

- Ein neues Abonnement erwerben - über diesen Link wird eine Bitdefender-Seite aufgerufen, über die Sie ein neues Abonnement erwerben können.
- Ich habe einen Aktivierungscode - über diesen Link wird Ihr Bitdefender Central-Konto aufgerufen. Das Fenster Meine Abonnements wird angezeigt. Klicken Sie hier auf **AKTIVIERUNGSCODE**. Geben Sie Ihren Aktivierungscode ein und klicken Sie auf **SENDEN**.

Klicken Sie auf **Fertigstellen**, um die Bitdefender Antivirus Plus 2016-Benutzeroberfläche aufzurufen.

3.2. Installation vom Installationsdatenträger

Um Bitdefender vom Installationsdatenträger aus zu installieren, legen Sie den Datenträger in das optische Laufwerk ein.

Ein Installationsbildschirm sollte nach wenigen Augenblicken angezeigt werden. Folgen Sie den Anweisungen, um die Installation zu starten.

Beachten Sie

Im Installationsbildschirm haben Sie die Möglichkeit, das Installationspaket vom Installationsdatenträger auf einen USB-Speicherstick zu kopieren. Dies kann sich als nützlich erweisen, wenn Sie Bitdefender auf einem Computer installieren wollen, der über kein Laufwerk verfügt (wie z.B. ein Netbook). Verbinden Sie das Speichermedium mit einem USB Port und klicken Sie auf **Kopiere auf USB**. Stecken Sie den Speicherstick anschließend in den USB-Port des Computers ohne Laufwerk und doppelklicken Sie in dem Ordner, in dem Sie das Installationspaket gespeichert haben, auf runsetup.exe.

Wenn der Installationsbildschirm nicht angezeigt wird, öffnen Sie im Windows Explorer das Root-Verzeichnis des Datenträgers und doppelklicken Sie auf autorun.exe.

Validierung der Installation

Bitdefender wird zuallererst Ihr System überprüfen, um die Installation zu bestätigen.

Wenn Ihr System die Mindestanforderungen zur Installation von Bitdefender nicht erfüllt, werden Sie darüber informiert, welche Bereiche aufgerüstet werden müssen, damit Sie fortfahren können.

Wenn ein inkompatibles Virenschutzprogramm oder eine ältere Version von Bitdefender erkannt wird, werden Sie aufgefordert, diese von Ihrem System zu entfernen. Bitte folgen Sie den Anweisungen, um die Software von Ihrem System zu entfernen und so spätere Probleme zu vermeiden. Unter Umständen müssen Sie Ihren Computer neu starten, um die Entfernung der erkannten Virenschutzprogramme abzuschließen.

Das Installationspaket für Bitdefender Antivirus Plus 2016 wird ständig aktualisiert. Klicken Sie dazu auf **Ja**, wenn Sie dazu aufgefordert werden. Bitdefender lädt dann die Dateien herunter und gewährleistet so, dass Sie die aktuelle Version der Software installieren.

Beachten Sie

Das Herunterladen der Installationsdateien kann eine Weile dauern, besonders bei langsameren Internetverbindungen.

Sobald die Installation validiert ist, startet der Installationsassistent. Folgen Sie den Schritten, um Bitdefender Antivirus Plus 2016 auf Ihrem PC zu installieren.

Schritt 1 - Installation von Bitdefender

Im Bitdefender-Installationsbildschirm können Sie entscheiden, welche Art von Installation Sie wünschen.

Wenn Sie sich nicht um Detaileinstellungen kümmern möchten, klicken Sie einfach auf **Installieren**. Bitdefender wird dann mit den Standardeinstellungen im Standardpfad installiert, und Sie können direkt mit Schritt 3 des Assistenten fortfahren.

Klicken Sie zur Konfiguration der Installationseinstellungen auf **Benutzerdef.**.

In diesem Schritt können Sie zwei zusätzliche Dinge tun:

- Lesen Sie vor der Installation die Endbenutzer-Lizenzvereinbarung. Die Lizenzvereinbarung enthält die Nutzungsbedingungen für Bitdefender Antivirus Plus 2016.

  Sollten Sie diesen Nutzungsbedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsprozess wird abgebrochen uns Sie verlassen den Assistenten.

- Wählen Sie **Berichte anonym senden** aus. Durch Aktivierung dieser Option, werden Berichte, die Informationen zu Ihrer Nutzung des Produktes enthalten, an Bitdefender Server gesendet. Diese Information ist wichtig für die Verbesserung des Produktes. Wir möchten Sie darauf hinweisen, dass diese Berichte keine vertraulichen Daten wie Ihren Namen oder Ihre IP-Adresse enthalten und dass diese Daten nicht für kommerzielle Zwecke verwendet werden.

Schritt 2 - Installation individuell anpassen

Beachten Sie

Dieser Schritt kommt nur dann vor, wenn Sie die benutzerdefinierte Installation gewählt haben.

Die folgenden Optionen sind verfügbar:

Installationspfad

Bitdefender Antivirus Plus 2016 wird standardmäßig im Ordner C:\Programme\Bitdefender\Bitdefender 2016 installiert. Falls Sie ein anderes Installationsverzeichnis wählen möchten, klicken Sie auf **Ändern** und wählen Sie das Verzeichnis, in dem Sie Bitdefender installieren möchten.

Proxy-Einstellungen konfigurieren

Bitdefender Antivirus Plus 2016 benötigt Zugriff auf das Internet, um die Produktaktivierung abzuschließen, Sicherheits- und Produkt-Updates herunterzuladen, In-the-Cloud-Komponenten zu nutzen usw. Wenn Sie eine Proxy-Verbindung anstelle einer direkten Internet-Verbindung nutzen, müssen Sie diese Option auswählen und die Proxy-Einstellungen konfigurieren.

Die Einstellungen können aus dem Standard-Browser importiert oder manuell eingegeben werden.

Klicken Sie auf **Installieren**, um Ihre Einstellungen zu bestätigen und mit der Installation zu beginnen. Wenn Sie sich später umentscheiden, können Sie einfach auf die entsprechende **Standard verwenden**-Schaltfläche klicken.

Schritt 3 - Installation wird durchgeführt

Bitte warten Sie, bis der Installationsvorgang abgeschlossen ist. Sie erhalten detaillierte Informationen über den Fortschritt der Installation.

Kritische Bereiche Ihres Systems werden nach Viren durchsucht, die neuesten Versionen der Anwendungsdateien heruntergeladen und installiert und die Bitdefender-Dienste gestartet. Dieser Schritt kann einige Minuten in Anspruch nehmen.

Schritt 4 - Installation ist abgeschlossen

Eine Zusammenfassung der Installation wird angezeigt. Sollte während der Installation aktive Malware erkannt und entfernt werden, könnte ein Neustart des Systems erforderlich werden. Klicken Sie auf **Weiter**.

Schritt 5 - Bitdefender Central

Nach Abschluss der ersten Einrichtung wird das Bitdefender Central-Fenster angezeigt. Zur Aktivierung des Produktes und zur Nutzung der

Online-Funktionen wird ein Bitdefender Central-Benutzerkonto benötigt. Für weitere Informationen lesen Sie bitte „*Bitdefender Central*“ (S. 40).

Fahren Sie entsprechend Ihrer Situation fort.

Ich habe bereits ein Bitdefender Central-Konto

Geben Sie die E-Mail-Adresse und das Passwort für Ihr Bitdefender Central-Benutzerkonto ein und klicken Sie auf **EINLOGGEN**.
Falls Sie das Passwort für Ihr Benutzerkonto vergessen haben oder Ihr bestehendes Passwort zurücksetzen möchten, klicken Sie auf den **Zurücksetzen des Passworts**-Link. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie danach auf **PASSWORT ZURÜCKSETZEN**.

Ich möchte ein Bitdefender Central-Konto anlegen

Klicken unten im Fenster auf **Anmelden**, um ein Bitdefender Central-Benutzerkonto anzulegen. Geben Sie die erforderlichen Informationen in die entsprechenden Felder ein und klicken Sie auf **BENUTZERKONTO ANLEGEN**.

Die hier eingetragenen Daten bleiben vertraulich.

Das Passwort muss mindestens 8 Zeichen lang sein und eine Zahl enthalten.

Beachten Sie

Sobald das Benutzerkonto angelegt wurde, können Sie sich mit der angegebenen E-Mail-Adresse und dem Passwort unter https://central.bitdefender.com bei Ihrem Konto anmelden.

Schritt 6 - Erste Schritte

Im Fenster "Erste Schritte" können Sie sehen, wie lange Ihr Abonnement noch gültig ist.

In diesem Schritt können Sie zwei zusätzliche Dinge tun:

- Ein neues Abonnement erwerben - über diesen Link wird eine Bitdefender-Seite aufgerufen, über die Sie ein neues Abonnement erwerben können.
- Ich habe einen Aktivierungscode - über diesen Link wird Ihr Bitdefender Central-Konto aufgerufen. Das Fenster Meine Abonnements wird angezeigt. Klicken Sie hier auf **AKTIVIERUNGSCODE**. Geben Sie Ihren Code ein und klicken Sie auf **SENDEN**.

Klicken Sie auf **Fertigstellen**, um die Bitdefender Antivirus Plus 2016-Benutzeroberfläche aufzurufen.

ERSTE SCHRITTE

4. GRUNDLAGEN

Nachdem Sie Bitdefender Antivirus Plus 2016 installiert haben, ist Ihr Computer geschützt gegen alle Arten von Malware (wie Viren, Spyware und Trojaner).

Die Anwendung nutzt die Photon-Technologie, um Malware-Scans zu beschleunigen und noch leistungsfähiger zu machen. Diese lernt, wie Sie die Anwendungen auf Ihrem System nutzen, und weiß so, was sie wann scannen soll. Dadurch werden die Auswirkungen auf die Systemleistung minimiert.

Sie können den Autopilot einschalten und beruhigt Sicherheit im Hintergrund genießen, ohne dass sie selbst irgendwelche Einstellungen vornehmen müssen. Sie können jedoch auch die Bitdefender-Einstellungen für die Feineinstellung nutzen und Ihren Schutz verbessern.

Bitdefender ermöglicht Ihnen ein störungsfreies Arbeiten, Spielen und Abspielen von Filmen, indem es Wartungsaufgaben aufschiebt, Unterbrechungen verhindert und die visuellen Einstellungen entsprechend anpasst. Sie können von all dem profitieren, indem Sie Ihre Profile aktivieren oder konfigurieren.

Bitdefender trifft alle sicherheitsrelevanten Entscheidungen für Sie und wird nur in seltenen Fällen Pop-up-Benachrichtigungen anzeigen. Nähere Informationen zu den durchgeführten Aktionen und zur Programmausführung finden Sie im Ereignisfenster. Für weitere Informationen lesen Sie bitte *„Ereignisanzeige“ (S. 18)*.

Von Zeit zu Zeit sollten Sie Bitdefender öffnen und existierende Probleme beheben. Es ist möglich, dass Sie, um Ihren Computer und Ihre Daten zu schützen, bestimmte Bitdefender-Komponenten konfigurieren oder vorbeugende Maßnahmen durchführen müssen.

Rufen Sie Ihr Bitdefender Central-Benutzerkonto auf, um die Online-Funktionen von Bitdefender Antivirus Plus 2016 zu nutzen und Ihre Abonnements und Geräte zu verwalten. Für weitere Informationen lesen Sie bitte *„Bitdefender Central“ (S. 40)*.

Im Abschnitt „Gewusst wie“ (S. 51) finden Sie detaillierte Anweisungen zur Ausführung der häufigsten Aufgaben. Wenn Sie bei der Verwendung von Bitdefender Probleme haben, finden Sie im Abschnitt *„Verbreitete Probleme beheben“ (S. 141)* Lösungen zu den häufigsten Problemen.

4.1. Das Bitdefender-Fenster öffnen

Um das Bitdefender Antivirus Plus 2016-Hauptfenster aufzurufen, gehen Sie folgendermaßen vor:

- In **Windows 7**:
  1. Klicken Sie auf **Start** und **Alle Programme**.
  2. Klicken Sie auf **Bitdefender 2016**.
  3. Klicken Sie auf **Bitdefender Antivirus Plus 2016**. Noch schneller geht es mit einem Doppelklick auf das Bitdefender-Symbol in der Task-Leiste.
- In **Windows 8 und Windows 8.1**:

  Finden Sie auf der Windows-Startseite Bitdefender Antivirus Plus 2016 (z.B. durch die Eingabe von "Bitdefender" auf der Startseite) und klicken Sie auf das entsprechende Symbol. Öffnen Sie alternativ die Desktop-App und doppelklicken Sie danach auf das Bitdefender-Symbol in der Task-Leiste.
- In **Windows 10**:

  Geben Sie im Suchfeld in der Taskleiste "Bitdefender" ein und klicken Sie auf das entsprechende Symbol. Alternativ ist auch ein Doppelklick auf das Bitdefender-Symbol in der Taskleiste möglich.

Weitere Informationen zum Bitdefender-Fenster und zum Symbol in der Task-Leiste finden Sie im Kapitel *„Bitdefender-Benutzeroberfläche“ (S. 27)*.

4.2. Probleme beheben

Bitdefender benutzt ein Problem-Tracking-System, um sicherheitsgefährdende Probleme festzustellen und Sie über diese zu informieren. Standardmässig wird nur ein Teil der für am wichtigsten erachteten Risiken überwacht. Sie können dies nach Bedarf verändern, wählen Sie aus über welche Risiken sie informiert werden möchten.

Zu den gefundenen Problemen gehören auch wichtige Schutzeinstellungen, die deaktiviert sind, und andere Umstände, die ein Sicherheitsrisiko darstellen. Sie sind in zwei Kategorien unterteilt:

- **Kritische Probleme** - Verhindern, dass Bitdefender Sie vor Malware schützt oder stellen ein erhebliches Sicherheitsrisiko dar.

- **Kleinere (nicht-kritische) Probleme** - Können Ihren Schutz in naher Zukunft beeinträchtigen.

Das Bitdefender-Symbol in der Task-Leiste weist Sie durch die folgenden Farbwechsel auf ausstehende Probleme hin:

Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.
Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.

Wenn Sie den Mauszeiger über das Symbol bewegen, wird Ihnen angezeigt, dass ein Problem existiert.

Nach dem Öffnen der Bitdefender-Benutzeroberfläche zeigt der Sicherheitsstatusbereich in der oberen Symbolleiste die Art der Probleme an, die Ihr System beeinträchtigen.

4.2.1. "Alle Probleme beheben"-Assistent

Um erkannte Probleme zu beheben, folgen Sie den Anweisungen des **Alle Probleme beheben**-Assistenten.

1. Befolgen Sie eine der folgenden Möglichkeiten, den Assistenten zu öffnen:
   - Rechtsklicken Sie auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie dann **Sicherheitsprobleme anzeigen**.
   - Öffnen Sie die Bitdefender-Benutzeroberfläche und klicken Sie auf eine beliebige Stelle innerhalb des Sicherheitsstatusbereichs in der oberen Symbolleiste (Sie können zum Beispiel auf die Schaltfläche **Alle Probleme beheben** klicken).
2. Sie erhalten eine Übersicht aller Probleme, die die Sicherheit Ihres Computers und Ihrer Daten beeinträchtigen. Alle aktuellen Probleme sind markiert und werden behoben.

   Wenn Sie ein bestimmtes Problem nicht sofort beheben möchten, deaktivieren Sie das entsprechende Kästchen. Sie werden aufgefordert anzugeben, für wie lange die Behebung des Problems verschoben werden soll. Wählen Sie die gewünschte Option aus dem Menü und klicken Sie auf **OK**. Um die Überwachung der jeweiligen Problemkategorie zu beenden, wählen Sie den Punkt **Dauerhaft**.

Der Status des Problems erscheint als **Aufgeschoben** und es wird keine Aktion zur Behebung des Problems durchgeführt.

3. Um die ausgewählten Probleme zu beheben, klicken Sie auf **Beheben**. Manche Probleme werden sofort behoben. Bei anderen hilft Ihnen ein Assistent bei der Behebung.

Die Risiken die Ihnen dieser Assistent hilft zu beheben, können in diese Hauptkategorien eingeordnet werden

- **Deaktivierte Sicherheitseinstellungen.** Solche Probleme werden sofort beseitigt, durch die entsprechenden Sicherheitseinstellungen.
- **Vorbeugende Sicherheitsaufgaben die Sie durchführen sollten.** Bei der Beseitigung solcher Probleme, hilft Ihnen ein Assistent.

4.2.2. Konfigurieren von Statusbenachrichtigungen

Bitdefender kann Sie informieren, wenn in einer der folgenden Komponenten ein Problem aufgetreten ist:

- Antivirus
- Update-Server
- Browser-Sicherheit

Sie können das Warnsystem ganz nach Ihren individuellen Ansprüchen konfigurieren, indem Sie wählen, über welche Ereignisse Sie informiert werden möchten. Folgen Sie diesen Schritten:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Erweitert** aus.
3. Klicken Sie auf **Statusbenachrichtigungen konfigurieren**.
4. Klicken Sie auf die Schalter, um die Statusbenachrichtigungen entsprechend Ihrer Anforderungen zu aktivieren oder zu deaktivieren.

4.3. Ereignisanzeige

Bitdefender führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer. Immer wenn etwas passiert, was die Sicherheit Ihres Systems oder ihrer Daten betrifft, wird in den Bitdefender-Ereignissen eine Nachricht erstellt, ähnlich einer neuen E-Mail in Ihrem Postfach.

Ereignisse sind ein wichtiges Hilfsmittel für die Überwachung und Verwaltung Ihres Bitdefender-Schutzes. So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem Computer entdeckt wurde usw. Zudem können Sie bei Bedarf weitere Aktionen ausführen oder die von Bitdefender ausgeführten Aktionen anpassen.

So öffnen Sie das Ereignisprotokoll:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.

Die Nachrichten werden nach dem Bitdefender-Modul sortiert, zu dem sie gehören:

- **Update-Server**
- **Antivirus**
- **Internet-Schutz**
- **Schwachstellen**
- **Ransomware-Schutz**

Bei jedem Ereignis wird über dem -Symbol oben rechts in der Bitdefender-Benutzeroberfläche ein Punkt angezeigt.

Eine Liste von Ereignissen ist für jede Kategorie verfügbar. Um Informationen über ein bestimmtes Ereignis in der Liste abzurufen, klicken Sie auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus. Ereignisdetails werden rechts im Fenster angezeigt. Sie erhalten die folgenden Informationen zu jedem Ereignis: eine Kurzbeschreibung; die Aktion, die Bitdefender beim Auftreten des Ereignisses durchgeführt hat; das Datum und der Zeitpunkt des Ereignisses. Unter Umständen werden Ihnen Optionen zur weiteren Vorgehensweise angeboten.

Sie können Ereignisse nach Wichtigkeit und nach Reihenfolge ihres Auftretens sortieren. Es gibt drei Arten von Ereignissen, die nach ihrer Wichtigkeit sortiert werden. Diese werden durch verschiedene Symbole unterschieden:

■ **Kritische** Ereignisse weisen auf kritische Probleme hin. Sie sollten sich umgehend darum kümmern.
■ **Warnung** Diese Ereignisse weisen auf nicht-kritische Probleme hin. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.

■ **Information** Diese Ereignisse weisen auf erfolgreich ausgeführte Vorgänge hin.

Um alle Ereignisse anzuzeigen, die über einem bestimmten Zeitraum aufgetreten sind, wählen Sie den gewünschten Zeitraum im entsprechenden Feld aus.

Um Ihnen die Verwaltung von protokollierten Ereignissen zu erleichtern, enthält jeder Abschnitt des Ereignisfensters Optionen, mit denen Sie alle Ereignisse in diesem Abschnitt löschen oder als gelesen markieren können.

4.4. Auto-Pilot

Für alle Benutzer, die nichts weiter von Ihrer Sicherheitslösung erwarten, als zuverlässigen Schutz, ohne bei der Arbeit gestört zu werden, bietet Bitdefender Antivirus Plus 2016 einen integrierten Autopilot-Modus.

Solange der Autopilot aktiviert ist, wird Bitdefender die optimale Sicherheitskonfiguration anwenden und alle sicherheitsrelevanten Entscheidungen für Sie treffen. Das bedeutet, dass keine Pop-ups oder Benachrichtigungen eingeblendet werden und Sie keinerlei Einstellungen vornehmen müssen.

Wenn der AutoPilot aktiviert ist, werden kritische Probleme von Bitdefender automatisch behoben. Zudem werden die folgenden Funktionen unauffällig im Hintergrund verwaltet:

- Virenschutz, gewährleistet durch Zugriff-Scans und ununterbrochenes Scanning.
- Internet-Schutz.
- Automatische Updates.

So schalten Sie den Autopiloten ein und aus:

1. Klicken Sie in der Symbolleiste oben in der Bitdefender-Benutzeroberfläche auf den **Autopilot**-Schalter.

Wenn der Autopilot eingeschaltet ist, erscheint folgendes Bitdefender-Symbol in der Task-Leiste: .

Wichtig

Wenn der Autopilot eingeschaltet ist und Sie eine der von ihm verwalteten Einstellungen verändern, wird er automatisch ausgeschaltet.

Um eine Übersicht der Aktionen anzuzeigen, die von Bitdefender durchgeführt wurden, während der Autopilot eingeschaltet war, öffnen Sie das Fenster Ereignisse.

4.5. Profile und Akkubetrieb

Bei einigen Aktivitäten am Computer, so zum Beispiel bei Online-Spielen oder Videopräsentationen, werden schnelle Reaktionszeiten und konstant hohe Systemleistung ohne Unterbrechungen benötigt. Wenn Ihr Laptop auf Batteriebetrieb läuft ist es ratsamer unnötige Vorgänge, welche zusätzlich Strom verbrauchen, zu verschieben, bis der Laptop extern mit Strom versorgt wird.

Um sich diesen besonderen Situationen anzupassen, hat Bitdefender Antivirus Plus 2016 zwei spezielle Betriebsmodi:

- Profile
- Akkubetrieb

4.5.1. Profile

Bitdefender-Profile weist den laufenden Anwendungen zusätzliche Systemressourcen zu, indem er die Schutzeinstellungen vorübergehend modifiziert und die Systemkonfiguration entsprechend anpasst. So werden die Systemauswirkungen auf Ihre jeweilige Aktivität minimiert.

Um den verschiedenen Aktivitäten gerecht zu werden, enthält Bitdefender die folgenden Profile:

Arbeitsprofil
: Sorgt für optimale Arbeitseffizienz, indem es die Produkt- und Systemeinstellungen erkennt und entsprechend anpasst.

Filmprofil
: Verbessert die visuellen Effekte und sorgt für störungsfreies Filmvergnügen.

Spielprofil
: Verbessert die visuellen Effekte und sorgt für störungsfreies Spielvergnügen.

Aktivieren und Deaktivieren von Profilen

So können Sie die Profile aktivieren oder deaktivieren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Wählen Sie im Fenster **Profile** den Reiter **Profileinstellungen** aus.
5. Aktivieren oder deaktivieren Sie die Profile, indem Sie auf den entsprechenden Schalter klicken.

Autopilot zur Überwachung der Profile konfigurieren

Für noch mehr Benutzerfreundlichkeit können Sie den Autopilot so konfigurieren, dass er Ihr Arbeitsprofil verwaltet. In diesem Modus erkennt Bitdefender automatisch Ihre jeweiligen Aktivitäten und optimiert den System- und Produktbetrieb entsprechend.

So konfigurieren Sie den Autopilot zur Verwaltung Ihrer Profile:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Wählen Sie im Fenster **Profile** den Reiter **Profileinstellungen** aus.
5. Aktivieren Sie das entsprechende **Autopilot soll meine Profile verwalten**-Kästchen.

Wenn Sie nicht möchten, dass Ihr Profil automatisch verwaltet wird, aktivieren Sie das Kästchen nicht und wählen Sie es manuell aus der **PROFILE**-Auswahlliste in der Bitdefender-Benutzeroberfläche aus.

Weitere Informationen zu Profilen finden Sie im Kapitel„*Profile*“ (S. 134)

4.5.2. Akkubetrieb

Der Akkubetrieb wurde speziell für Laptop- und Tablet-Nutzer entwickelt. Er minimiert die Auswirkungen des System- und Bitdefender-Betriebs auf die Akkulaufzeit, sobald der von Ihnen festgelegte Akkuladestand unterschritten wird.

Die folgenden Produkteinstellungen werden angewendet, wenn Bitdefender in den Akkubetrieb versetzt wird:

- Automatische Bitdefender-Updates werden verschoben.
- Geplante Scans werden verschoben.
- Das Sicherheits-Widget wird deaktiviert.

Bitdefender erkennt, wenn Ihr Laptop vom Stromnetz getrennt wird und startet den Akkubetrieb automatisch je nach festgelegten Akkuladestand. Ebenso beendet Bitdefender automatisch den Akkubetrieb, wenn der Laptop nicht mehr über den Akku betrieben wird.

So können Sie den Akkubetrieb aktivieren oder deaktivieren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Wählen Sie im Modul **Profile** den Reiter **Akkubetrieb** aus.
4. Aktivieren oder deaktivieren Sie den automatischen Akkubetrieb, indem Sie auf den entsprechenden Schalter klicken.

   Schieben Sie den entsprechenden Regler auf den Wert, bei dem das System in den Akkubetrieb wechseln soll. Standardmäßig wird der Akkubetrieb aktiviert, sobald der Akkuladestand unter 30 % sinkt.

Beachten Sie
Der Akkubetrieb ist auf Laptops und Tablets standardmäßig aktiviert.

Konfigurieren des Akkubetriebs

So konfigurieren Sie den Akkubetrieb:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Wählen Sie im Modul **Profile** den Reiter **Akkubetrieb** aus.
4. Aktivieren Sie die Funktion, indem Sie auf den entsprechenden Schalter klicken.
5. Klicken Sie auf die Schaltfläche **Konfigurieren**.

6. Wählen Sie die durchzuführenden Systemanpassungen aus, indem Sie die folgenden Optionen auswählen:
   - Produkteinstellungen für den Akkubetrieb optimieren.
   - Hintergrundprogramme und Wartungsaufgaben verschieben.
   - Automatische Windows-Updates später durchführen.
   - Energiesparplaneinstellungen für den Akkubetrieb anpassen.
   - Externe Geräte und Netzwerk-Ports deaktivieren.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

4.6. Passwortschutz für Bitdefender-Einstellungen

Wenn Sie nicht der einzige Benutzer des Computers sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen mit einem Passwort zu schützen.

Um den Passwortschutz für die Bitdefender-Einstellungen zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
3. Aktivieren Sie den Passwortschutz, indem Sie auf den entsprechenden Schalter klicken.
4. Geben Sie das Passwort in die beiden Felder ein und klicken Sie dann auf **OK**. Das Passwort muss mindestens 8 Zeichen lang sein.

Sobald Sie ein Passwort festgelegt haben, muss jeder, der die Bitdefender-Einstellungen verändern will, zunächst das Passwort eingeben.

> **Wichtig**
>
> Merken Sie sich Ihr Passwort gut oder schreiben Sie es auf und verwahren es an einem sicheren Platz. Wenn Sie Ihr Passwort vergessen haben, müssen Sie das Programm neu installieren oder den Kundendienst von Bitdefender kontaktieren.

Um den Passwortschutz zu deaktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
3. Deaktivieren Sie den Passwortschutz, indem Sie auf den Schalter klicken. Geben Sie das Passwort ein und klicken Sie auf **OK**.

Beachten Sie
Um das Passwort für Ihr Produkt zu ändern, klicken Sie auf **Passwort ändern**.

4.7. Anonyme Nutzungsberichte

Bitdefender verschickt standardmäßig Berichte mit Nutzungsinformationen an die Bitdefender-Server. Diese Information ist wichtig für die Verbesserung des Produktes. Bitte beachten Sie, dass diese Berichte weder vertrauliche Daten, wie Ihren Namen und Ihre IP Adresse, enthalten, noch werden diese Daten für kommerzielle Zwecke verwendet.

Wenn Sie das Versenden von anonymen Nutzungsberichten beenden wollen, gehen Sie folgendermaßen vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Erweitert** aus.
3. Klicken Sie auf den Schalter, um anonyme Nutzungsberichte auszuschalten.

4.8. Sonderangebote und Produktbenachrichtigungen

Sind Sonderangebote verfügbar, wird das Bitdefender-Produkt Sie per Pop-up-Benachrichtigung darüber informieren. So können Sie von unseren Vorteilspreisen profitieren und Ihre Geräte länger schützen.

Zudem können Produktbenachrichtigungen angezeigt werden, wenn der Benutzer Veränderungen im Produkt vornimmt.

So können Sie Benachrichtigungen zu Sonderangeboten und dem Produkt aktivieren oder deaktivieren:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
3. Aktivieren oder deaktivieren Sie Benachrichtigungen zu Sonderangeboten und dem Produkt, indem Sie auf den entsprechenden Schalter klicken.

Die Option für die Benachrichtigungen zu Sonderangeboten und dem Produkt ist standardmäßig aktiviert.

Beachten Sie

Wenn Sie die Benachrichtigungen zu Sonderangeboten und dem Produkt deaktivieren, wird Bitdefender Sie auch weiterhin über Sonderangebote informieren, falls Sie eine Testversion nutzen, Ihre Lizenz in Kürze abläuft oder Sie eine bereits abgelaufene Produktversion nutzen.

5. BITDEFENDER-BENUTZEROBERFLÄCHE

Bitdefender Antivirus Plus 2016 entspricht den Bedürfnissen sowohl von Profis als auch von Beginnern. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.

Um den Produktstatus abzurufen und grundlegende Aufgaben auszuführen, steht Ihnen das Bitdefender-Symbol in der Task-Leiste jederzeit zur Verfügung.

Über das Hauptfenster haben Sie Zugriff auf wichtige Produktinformationen und die einzelnen Produktmodule und können die häufigsten Aufgaben erledigen. Über das Hauptfenster können Sie für eine detaillierte Konfiguration und erweiterte Verwaltungsaufgaben auf die Bitdefender-Module zugreifen und mittels des Autopiloten und der Profile das Produktverhalten konfigurieren.

Wenn Sie wichtige Sicherheitsinformationen ständig im Blick haben und direkten Zugriff auf wichtige Einstellungen haben möchten, können Sie das Sicherheits-Widget zu Ihrem Desktop hinzufügen.

5.1. Task-Leisten-Symbol

Um das gesamte Produkt schneller zu verwalten, können Sie das Bitdefender-Symbol in der Task-Leiste nutzen.

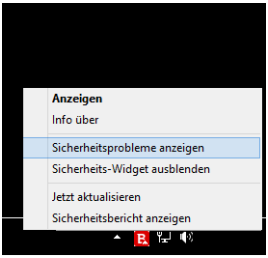
Beachten Sie

Das Bitdefender-Symbol ist unter Umständen nicht immer sichtbar. So können Sie das Symbol immer sichtbar halten:

- In **Windows 7, Windows 8 und Windows 8.1**:
  1. Klicken Sie auf den Pfeil in der unteren rechten Ecke des Bildschirms.
  2. Klicken Sie auf **Benutzerdefiniert ...**, um das Fenster der Infobereichsymbole zu öffnen.
  3. Wählen Sie **Symbole und Benachrichtigungen anzeigen** für das Symbol **Bitdefender Agent**.
- In **Windows 10**:
  1. Rechtsklicken Sie auf der Leiste und wählen Sie **Eigenschaften**.
  2. Klicken Sie im Fenster der Taskleiste auf **Anpassen**.

3. Klicken Sie im Fenster **Benachrichtigungen & Aktionen** auf den Link **Klicken Sie hier, um die Symbole auszuwählen, die auf der Taskleiste angezeigt werden.**.
4. Aktivieren Sie den Schalter neben **Bitdefender-Agent**.

Wenn Sie dieses Icon doppelklicken wird sich Bitdefender öffnen. Wird das Symbol mit der rechten Maustaste angeklickt, öffnet sich ein Kontextmenü, mit dem Sie das BitdefenderProdukt verwalten können.



Taskleistensymbol

- **Anzeigen** - Öffnet das Bitdefender-Hauptfenster.
- **Über** - öffnet ein Fenster, in dem Sie Informationen über Bitdefender erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht.
- **Sicherheitsprobleme anzeigen** - hilft bestehende Sicherheitsschwachstellen zu entfernen. Falls die Option nicht verfügbar ist, so gibt es keine zu behebenden Probleme. Für weitere Informationen lesen Sie bitte *„Probleme beheben“ (S. 16)*.
- **Sicherheits-Widget anzeigen/ausblenden** - aktiviert/deaktiviert das Sicherheits-Widget.
- **Jetzt Aktualisieren** - startet ein sofortiges Update. Sie können den Update-Status im Update-Bereich des Bitdefender Hauptfensters verfolgen.
- **Sicherheitsbericht anzeigen** - Öffnet ein Fenster, in dem ein wöchentlicher Statusbericht sowie Empfehlungen für Ihr System angezeigt werden. Beachten Sie die Empfehlungen, um die Sicherheit Ihres Systems zu verbessern.

Das Bitdefender-Symbol in der System Tray informiert Sie über spezielle Symbole, über mögliche Probleme:

Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.
Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
Der Bitdefender-Autopilot ist aktiviert.

Wenn Bitdefender nicht aktiv ist, ist das Symbol in der Task-Leiste grau hinterlegt: . Dies passiert normalerweise, wenn die Lizenz abgelaufen ist. Es kann auch vorkommen, wenn die Bitdefender Services nicht reagieren oder andere Fehler die normale Funktionsweise von Bitdefender einschränken.

5.2. Hauptfenster

Im Bitdefender-Hauptfenster können Sie die häufigsten Aufgaben durchführen, Sicherheitsprobleme schnell und einfach beheben, Informationen über die Programmausführung anzeigen und auf die verschiedenen Bereiche zugreifen, über die sich die Produkteinstellungen konfigurieren lassen. Und das alles mit nur wenigen Klicks.

Das Fenster ist in zwei Hauptbereiche aufgeteilt:

Obere Symbolleiste
: Hier können Sie den Sicherheitsstatus Ihres Computers überprüfen, das Bitdefender-Verhalten in bestimmten Situationen konfigurieren und auf wichtige Aufgaben zugreifen.

Schaltflächenbereich
: Hier können Sie das Bitdefender Central-Dashboard aufrufen und verschiedene Aufgaben ausführen, um Ihren Computer zu schützen und die Systemgeschwindigkeit zu optimieren.

Über das -Symbol unten links im Hauptfenster können Sie auf die Produktmodule zugreifen, um mit der Konfiguration der Produkteinstellungen zu beginnen.

Über das -Symbol im oberen Bereich des Hauptfensters können Sie Ihr Konto verwalten und über das Konto-Dashboard auf die Online-Funktionen des Produkts zugreifen. Von hier aus können Sie auch die Ereignisanzeige, den wöchentlichen Sicherheitsbericht und die Hilfe & Support-Seite aufrufen.

Link	Beschreibung
Anzahl der verbleibenden Tage	Der Zeitraum bis zum Ablauf Ihres aktuellen Abonnements wird angezeigt. Wenn Sie auf den Link klicken, wird ein Fenster geöffnet, in dem mehr Informationen über Ihren Lizenzschlüssel angezeigt werden und in dem Sie Ihr Produkt mit einem neuen Lizenzschlüssel registrieren können.

5.2.1. Obere Symbolleiste

Die obere Symbolleiste enthält die folgenden Elemente:

- **Sicherheitsstatusbereich** Dieser befindet sich auf der linken Seite der Symbolleiste und enthält Informationen darüber, ob Probleme die Sicherheit Ihres Computers beeinträchtigen und hilft Ihnen, diese zu beheben.

  Die Farbe des Sicherheitsstatusbereichs verändert sich abhängig von den erkannten Problemen. Zudem werden unterschiedliche Meldungen angezeigt:

  - **Der Bereich ist grün markiert.** Es müssen keine Probleme behoben werden. Ihr Rechner und Ihre Daten sind geschützt.
  - **Der Bereich ist gelb markiert.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
  - **Der Bereich ist rot markiert.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie sollten sich umgehend um diese Probleme kümmern.

  Mit einem Klick auf eine beliebige Stelle im Sicherheitsstatusbereich können Sie einen Assistenten aufrufen, mit dem Sie alle Bedrohungen einfach und schnell von Ihrem Computer entfernen können. Für weitere Informationen lesen Sie bitte *„Probleme beheben“* (S. 16).

- **Autopilot** Hier können Sie den Autopilot aktivieren und den unauffälligen Hintergrundschutz für sich arbeiten lassen. Für weitere Informationen lesen Sie bitte *„Auto-Pilot“* (S. 20).
- **Profile** Hier können Sie das System so konfigurieren, dass Wartungsaufgaben automatisch verschoben werden, damit Sie unterbrechungsfrei arbeiten, spielen und Filme ansehen können. Für weitere Informationen lesen Sie bitte *„Profile“* (S. 134).

5.2.2. Schaltflächen

Über die Schaltflächen können Sie bequem auf Ihr Bitdefender Central-Benutzerkonto zugreifen und wichtige Aufgaben starten.

In diesem Bereich stehen Ihnen die folgenden Schaltflächen zur Verfügung:

- **Zu Bitdefender Central**. In Ihrem Bitdefender Central-Konto können Sie Ihre Abonnements einsehen und auf den von Ihnen verwalteten Geräten Sicherheitsaufgaben ausführen.
- **Quick-Scan**. Führen Sie einen Quick Scan durch, um sicherzustellen, dass Ihr Computer virenfrei ist.
- **Schwachstellen-Scan**. Überprüfen Sie Ihren Computer nach Schwachstellen, um sicherzustellen, dass alle installierten Anwendungen und Ihr Betriebssystem auf dem neuesten Stand sind und ordnungsgemäß laufen.
- **Safepay**. Öffnen Sie Bitdefender Safepay™, um Ihre sensiblen Daten bei Online-Transaktionen zu schützen.
- **Update**. Aktualisieren Sie Ihr Bitdefender, um sicherzustellen, dass Ihre Malware-Signaturen auf dem neuesten Stand sind.

5.3. Die Bitdefender-Module

Das Bitdefender-Produkt enthält eine Reihe nützlicher Module, um Sie bei der Arbeit, beim Surfen im Internet, beim Spielen oder bei der Abwicklung von Online-Zahlungen zu schützen.

Klicken Sie unten links im Bitdefender-Fenster auf das -Symbol, um auf die Module zuzugreifen oder das Produkt zu konfigurieren,

Die Module sind anhand ihrer Funktionen in drei Bereiche aufgeteilt:

- Schutz
- Privatsphäre
- Extras

5.3.1. Schutz

In diesem Bereich können Sie die Sicherheitsstufe konfigurieren und festlegen, welche Schwachstellen im System behoben werden sollen.

Im Bereich Schutz können Sie die folgenden Module verwalten:

Antivirus

Der Virenschutz bildet die Grundlage Ihrer Sicherheit. Bitdefender schützt Sie sowohl in Echtzeit als auch bei Bedarf vor allen Arten von Malware, so zum Beispiel vor Viren, Trojanern, Spyware, Adware usw.

Über das Modul Virenschutz können Sie schnell und einfach auf die folgenden Scan-Aufgaben zugreifen:

- Quick-Scan
- System-Scan
- Scans verwalten
- Rettungsmodus

Weitere Informationen zu den Scan-Aufgaben und eine Anleitung, wie Sie den Virenschutz konfigurieren können, finden Sie im Kapitel *„Virenschutz“* (S. 78).

Internet-Schutz

Mit dem Internet-Schutz schützen Sie sich beim Surfen zuverlässig vor Phishing-Angriffen, Betrugsversuchen und der unbeabsichtigten Weitergabe privater Daten.

Weitere Informationen, wie man Bitdefender zum Schutz Ihrer Internet-Aktivitäten konfigurieren kann, finden Sie im Kapitel *„Internet-Schutz“* (S. 105).

Schwachstellen

Über das Schwachstellen-Modul halten Sie Ihr Betriebssystem und Ihre regelmäßig genutzten Anwendungen auf dem neusten Stand.

Klicken Sie im Modul Schwachstellen auf **Schwachstellen-Scan**, um kritische Windows-Updates, Anwendungs-Updates und schwache Passwörter für Windows-Konten zu identifizieren.

Weitere Informationen zur Konfiguration des Schwachstellenschutzes finden Sie im Kapitel *„Schwachstellen“* (S. 110).

Ransomware-Schutz

Das Modul für den Ransomware-Schutz schützt Ihre persönlichen Dateien zuverlässig vor Angriffen von Online-Kriminellen.

Weitere Informationen zur Konfiguration des Ransomware-Schutzes zur Abwehr von Ransomware-Angriffen finden Sie im Kapitel *„Ransomware-Schutz“* (S. 114).

5.3.2. Privatsphäre

Im Bereich Privatsphäre können Sie Ihre Online-Transaktionen schützen und Ihr Surf-Vergnügen absichern.

Im Bereich Privatsphäre können Sie die folgenden Module verwalten:

Identitätsschutz

Mit dem Datenschutzmodul können Sie Dateien dauerhaft löschen.

Klicken Sie im Modul Datenschutz auf **Dateischredder**, um einen Assistenten zu starten, mit dem Sie Dateien endgültig von Ihrem System entfernen können.

Weitere Informationen zur Konfiguration des Datenschutzes finden Sie im Kapitel *„Identitätsschutz“* (S. 108).

Passwortmanager

Der Bitdefender-Passwortmanager hilft Ihnen, nie wieder ein Passwort zu vergessen. Zudem schützt er Ihre Privatsphäre und garantiert ein sicheres Internet-Vergnügen.

Im Passwortmanager-Modul können Sie die folgenden Aufgaben auswählen:

- **Geldbörse öffnen** - Öffnet die bestehende Geldbörse-Datenbank.
- **Geldbörse sperren** - Sperrt die bestehende Geldbörse-Datenbank.
- **Geldbörse exportieren** - Hiermit können Sie die bestehende Datenbank lokal speichern.
- **Neue Geldbörse anlegen** - Öffnet einen Assistenten, mit dem Sie eine neue Geldbörse-Datenbank anlegen können.

Weitere Informationen über die Konfiguration des Passwortmanagers finden Sie im Kapitel *„Passwortmanager-Schutz für Ihre Anmeldedaten“* (S. 123).

Safepay

Mit dem Bitdefender Safepay™-Browser können Sie Ihre Online-Bankgeschäfte und -Einkäufe und alle anderen Online-Transaktionen absichern und vor fremden Zugriff schützen.

Klicken Sie im Bitdefender-Hauptfenster auf die **Safepay**-Schaltfläche, um Ihre Online-Transaktionen in einer sicheren Umgebung abzuwickeln.

Weitere Informationen zu Bitdefender Safepay™ finden Sie im Kapitel *„Sichere Online-Transaktionen mit Safepay“* (S. 118).

5.3.3. Extras

Im Bereich Extras können Sie Ihr Arbeitsprofil konfigurieren.

Im Bereich Extras können Sie die folgenden Module verwalten:

Profile

Die Bitdefender-Profile überwachen den Produkt- und Systembetrieb und sorgen so für mehr Benutzerfreundlichkeit, wenn Sie arbeiten, spielen oder Filme schauen. Klicken Sie in der oberen Symbolleiste in der Bitdefender-Benutzeroberfläche auf **Jetzt aktivieren**, um diese Funktion zu nutzen.

Mit Bitdefender können Sie die folgenden Profile konfigurieren:

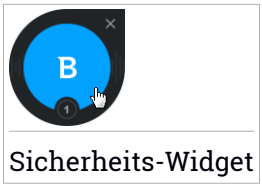
- Arbeitsprofil
- Filmprofil
- Spielprofil

Weitere Informationen zur Konfiguration des Moduls Profile finden Sie in Kapitel *„Profile“* (S. 134).

5.4. Sicherheits-Widget

Das **Sicherheits-Widget** ist die bequemste und schnellste Art Bitdefender Antivirus Plus 2016 zu steuern. Wenn Sie dieses kleine, unauffällige Widget auf Ihren Desktop legen, haben Sie jederzeit wichtige Informationen im Blick und können zentrale Aufgaben ausführen:

- Öffnet das Bitdefender-Hauptfenster.
- Scan-Activität in Echtzeit überwachen;
- den Sicherheitsstatus Ihres Systems überwachen und gefundene Probleme beheben;
- Zeigt an, wenn ein Update durchgeführt wird.
- Benachrichtigungen und Ereignisprotokolle von Bitdefender lesen;
- Dateien und Ordner (einzeln oder als Gruppe) scannen, indem Sie sie auf das Widget ziehen;



Sicherheits-Widget

Der Gesamtsicherheitsstatus Ihres Computers wird **in der Mitte** des Widgets angezeigt. Farbe und Form des Symbols in der Mitte zeigen unterschiedliche Status an.

Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt.

Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden. Klicken Sie auf das Statussymbol, um die gemeldeten Probleme zu beheben.

Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben. Klicken Sie auf das Statussymbol, um die gemeldeten Probleme zu beheben.

Ihr System ist geschützt.

Während ein Bedarf-Scan läuft, wird dieses animierte Symbol angezeigt.

Wenn Probleme gemeldet werden, klicken Sie auf das Statussymbol, um den Problembehebungsassistenten zu starten.

Im unteren Bereich des Widgets werden die ungelesenen Ereignisse angezeigt (die Anzahl der unbeachteten Ereignisse, die Bitdefender gemeldet hat). Klicken Sie auf den Ereigniszähler, der z. B. bei einem ungelesenen Ereignis so aussieht, um das Ereignisfenster zu öffnen. Für weitere Informationen lesen Sie bitte *„Ereignisanzeige“ (S. 18)*.

5.4.1. Dateien und Verzeichnis scannen

Mit dem Sicherheits-Widget können Sie ganz einfach Dateien und Ordner scannen. Sie können Dateien und/oder Ordner einfach auf das **Sicherheits-Widget** ziehen und dort ablegen, um diese(n) Datei/Ordner zu scannen.

Der Viren-Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang. Die Scan-Optionen sind für bestmögliche Erkennungsraten vorkonfiguriert und können nicht verändert werden. Falls infizierte Dateien gefunden werden, wird Bitdefender versuchen, diese zu desinfizieren (den Schad-Code zu entfernen). Wenn die Desinfizierung fehlschlagen sollte, wird Ihnen der Viren-Scan-Assistent andere Möglichkeiten anbieten, wie mit den infizierten Dateien verfahren werden soll.

5.4.2. Das Sicherheits-Widget ausblenden/anzeigen

Wenn Sie das Widget nicht mehr angezeigt bekommen möchten, klicken Sie einfach auf ⊗.

Verwenden Sie eine der folgenden Methoden, um das Sicherheits-Widget wiederherzustellen:

- Über die Task-Leiste:
  1. Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Task-Leiste.
  2. Klicken Sie im daraufhin angezeigten Kontextmenü auf **Sicherheits-Widget anzeigen**.
- Über die Bitdefender-Benutzeroberfläche:
  1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
  2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
  3. Aktivieren Sie den **Sicherheits-Widget anzeigen**, indem Sie auf den entsprechenden Schalter klicken.

5.5. Sicherheitsbericht

Der Sicherheitsbericht liefert Ihnen neben einem wöchentlichen Produktstatus verschiedene Tipps zur Verbesserung des Systemschutzes. Diese Tipps sind eine wichtige Hilfe bei der Verwaltung Ihres Schutzes und ermöglichen einen schnellen Überblick über die verfügbaren Aktionen.

Der Bericht wird einmal pro Woche erstellt und fasst alle relevanten Informationen zu den Produktaktivitäten zusammen, um Ihnen einen schnellen Überblick über alle Ereignisse in diesem Zeitraum zu geben.

Die Informationen im Sicherheitsbericht sind in zwei Kategorien unterteilt:

- Der Bereich **Schutz** - Zeigt Informationen zum Thema Systemschutz an.
  - **Geprüfte Spy-Dateien**

    Hier sehen Sie die Dateien, die von Bitdefender im Verlauf der Woche gescannt wurden. Hier können Sie alle Details wie die Anzahl der gescannten Dateien und der von Bitdefender bereinigten Dateien einsehen.

    Weitere Informationen zum Virenschutz finden Sie im Kapitel „*Virenschutz*“ (S. 78).
  - **Gescannte Websites**

    Hier können Sie sehen, wie viele Webseiten von Bitdefender gescannt und blockiert wurden. Um Sie vor der Preisgabe von persönlichen Informationen im Internet zu schützen, sichert Bitdefender Ihren Datenverkehr ab.

    Weitere Informationen zum Internet-Schutz finden Sie im Kapitel „*Internet-Schutz*“ (S. 105)
  - **Schwachstellen**

    Hier können Sie Systemschwachstellen schnell und einfach identifizieren und beheben, um Ihren Computer besser vor Malware und Hacker-Angriffen zu schützen.

    Weitere Informationen zum Schwachstellen-Scan finden Sie im Kapitel „*Schwachstellen*“ (S. 110).
  - **Ereignischronik**

    Hier können Sie sich einen Überblick über alle Scan-Prozesse und von Bitdefender im Laufe der Woche behobenen Probleme verschaffen. Die Ereignisse sind nach Tagen geordnet.

    Weitere Informationen und ein detailliertes Ereignisprotokoll aller Aktivitäten auf Ihrem Computer finden Sie unter Ereignisse.

- **Optimierungs**bereich - Hier erhalten Sie Informationen zu gewonnenen Speicherplatz, optimierten Anwendungen und der Akkulaufzeit, die Sie durch den Akkubetrieb gewonnen haben.
  - **Gewonnene Akkulaufzeit**

    Hier können Sie sehen, wie viel Akkulaufzeit Sie durch den Akkubetrieb gewonnen haben.

    Weitere Informationen zum Akkubetrieb finden Sie im Kapitel *„Akkubetrieb“* (S. 22).
  - **Optimierte Apps**

    Hier sehen Sie die Anzahl der Anwendungen, die Sie im Zusammenhang mit den Profilen verwendet haben.

    Weitere Informationen zur Profile finden Sie im Kapitel *„Profile“* (S. 134).

5.5.1. Aufrufen des Sicherheitsberichts

Der Sicherheitsbericht nutzt ein System zur Problemverfolgung, um potenzielle Sicherheitsprobleme für Ihren Computer und Ihre Daten zu erkennen und Sie darüber zu informieren. Zu den gefundenen Problemen gehören auch wichtige Schutzeinstellungen, die deaktiviert sind, und andere Umstände, die ein Sicherheitsrisiko darstellen. Mithilfe des Berichts können Sie bestimmte Bitdefender-Komponenten konfigurieren oder vorbeugende Maßnahmen ergreifen, um Ihren Computer und Ihre privaten Daten zu schützen.

Um den Sicherheitsbericht aufzurufen, gehen Sie folgendermaßen vor:

1. Den Bericht öffnen:
   - Klicken Sie oben im Bitdefender-Hauptfenster auf das -Symbol und wählen Sie **Sicherheitsbericht** aus dem Menü aus.
   - Rechtsklicken Sie auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie **Sicherheitsbericht anzeigen**.
   - Sie erhalten eine Pop-up-Benachrichtigung sobald ein Bericht bereitsteht. Klicken Sie auf **Anzeigen**, um den Sicherheitsbericht aufzurufen.

     In Ihrem Browser wird eine Seite geöffnet, auf der Sie den erstellten Bericht einsehen können.
2. Im Fenster oben können Sie den allgemeinen Sicherheitsstatus einsehen.

3. Lesen Sie unsere Empfehlungen unten auf der Seite.

Die Farbe des Sicherheitsstatusbereichs verändert sich abhängig von den erkannten Problemen. Zudem werden unterschiedliche Meldungen angezeigt:

- **Der Bereich ist grün markiert.** Es müssen keine Probleme behoben werden. Ihr Rechner und Ihre Daten sind geschützt.
- **Der Bereich ist gelb markiert.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
- **Der Bereich ist rot markiert.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie sollten sich umgehend um diese Probleme kümmern.

5.5.2. Aktivieren oder Deaktivieren der Benachrichtigungen zum Sicherheitsbericht

Um die Benachrichtigungen zum Sicherheitsbericht zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Allgemeine Einstellungen** aus.
3. Klicken Sie auf den entsprechenden Schalter, um die Benachrichtigungen zum Sicherheitsbericht zu aktivieren oder deaktivieren.

   Die Benachrichtigungen zum Sicherheitsbericht sind standardmäßig aktiviert.

6. BITDEFENDER CENTRAL

Bitdefender Central stellt Ihnen eine Web-Plattform zur Verfügung, über die Sie auf die Online-Funktionen und -Dienste des Produkts zugreifen und wichtige Aufgaben auf allen Geräten ausführen können, auf denen Bitdefender installiert ist. Über https://central.bitdefender.com können Sie sich mit jedem internetfähigen Computer oder Mobilgerät bei Ihrem Bitdefender Central-Konto anmelden. Nachdem Sie es aufgerufen haben, stehen Ihnen die folgenden Optionen zur Verfügung:

- Laden Sie Bitdefender herunter und installieren Sie es auf Windows-, OS X- und Android-Betriebssystemen. Die folgenden Produkte stehen zum Download bereit:
  - Bitdefender Antivirus Plus 2016
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security
- Verwaltung und Verlängerung Ihrer Bitdefender-Abonnements.
- Hinzufügen neuer Geräte zu Ihrem Netzwerk und Fernverwaltung dieser Geräte.

6.1. Aufrufen Ihres Bitdefender Central-Benutzerkontos.

Es gibt verschiedene Möglichkeiten, Ihr Bitdefender Central-Konto aufzurufen. Je nach durchzuführender Aufgabe stehen Ihnen die folgenden Optionen zur Verfügung:

- Über das Bitdefender-Hauptfenster:
  1. Klicken Sie links im Bitdefender-Fenster auf **Bitdefender Central besuchen**.
- Über die Kontodetails:
  1. Klicken Sie oben in der Bitdefender-Fenster auf das -Symbol und wählen Sie **Kontodetails** aus dem Menü aus.
  2. Ein neues Fenster wird angezeigt. Klicken Sie hier auf den **Bitdefender Central besuchen**-Link.

- Über Ihren Web-Browser:
  1. Öffnen Sie einen Web-Browser auf jedem beliebigen internetfähigen Gerät.
  2. Gehen Sie zu: https://central.bitdefender.com.
  3. Melden Sie sich mit Ihre E-Mail-Adresse und Passwort bei Ihrem Konto an.

6.2. Meine Abonnements

Über die Bitdefender Central-Plattform können Sie bequem die Abonnements für alle Ihre Geräte verwalten.

6.2.1. Verfügbare Abonnements anzeigen

So können Sie Ihre verfügbaren Abonnements anzeigen:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Abonnements** auf.

Hier werden alle Informationen zur Verfügbarkeit Ihrer Abonnements und die Anzahl der Geräte angezeigt, auf denen diese verwendet werden.

Klicken Sie auf eine Abonnementkarte, um Ihrem Abonnement ein neues Gerät hinzuzufügen oder es zu verlängern.

Beachten Sie
Sie können in Ihrem Konto auch mehrere Abonnements verwalten, vorausgesetzt, dass es sich dabei um Abonnements für unterschiedliche Produkte handelt.

6.2.2. Ein neues Gerät hinzufügen

Falls Ihr Abonnement mehr als ein Gerät umfasst, können Sie ein neues Gerät hinzufügen und darauf Ihr Bitdefender Antivirus Plus 2016 installieren. Gehen Sie dazu wie folgt vor:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie im Fenster **Meine Geräte** auf **Bitdefender installieren**.
4. Wählen Sie zunächst **Windows** und danach eine der beiden Optionen aus:

- Ich möchte Bitdefender **Auf diesem Gerät** installieren.

  Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus und klicken Sie auf **Herunterladen**, um fortzufahren.

- Ich möchte Bitdefender **Auf einem anderen Gerät** installieren.

  Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.

5. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

6.2.3. Abonnement verlängern

Falls Sie sich nicht für eine automatische Verlängerung Ihres Bitdefender-Abonnements entschieden haben, können Sie es auch selbst verlängern. Gehen Sie dazu wie folgt vor:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Abonnements** auf.
3. Wählen Sie die gewünschte Abonnementkarte aus.
4. Klicken Sie zum Fortfahren auf **Verlängern**.

In Ihrem Web-Browser wird eine neue Seite geöffnet, über die Sie Ihr Bitdefender-Abonnement verlängern können.

6.2.4. Abonnement aktivieren

Sie können Ihr Abonnement während des Installationsvorgangs mithilfe Ihres Bitdefender Central-Kontos aktivieren. Der Gültigkeitszeitraum beginnt mit dem Zeitpunkt der Aktivierung.

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer Ihres Bitdefender-Abonnements um dieses Zeitraum verlängern, vorausgesetzt es handelt sich um einen Code für das gleich Produkt.

So können Sie Ihr Abonnement mit einem Aktivierungscode aktivieren:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Abonnements** auf.

3. Klicken Sie auf **AKTIVIERUNGSCODE** und geben Sie den Code in das entsprechende Feld ein.
4. Klicken Sie auf **SENDEN**.

Das Abonnement wurde aktiviert. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **Bitdefender INSTALLIEREN**, um das Produkt auf einem Ihrer Geräte zu installieren.

6.3. Meine Geräte

Über Ihr Bitdefender Central-Benutzerkonto können Sie im Bereich **Meine Geräte** die Bitdefender-Produkte auf Ihren Geräten verwalten, vorausgesetzt, diese sind eingeschaltet und mit dem Internet verbunden. Auf der Gerätekarte werden der Name des Gerätes, sein Sicherheitsstaus und die verbleibende Gültigkeitsdauer des Abonnements angezeigt.

Sie können Gerätenamen vergeben, um die Geräte später leichter identifizieren zu können:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf das ⋮ -Symbol auf der gewünschten Gerätekarte und wählen Sie **Einstellungen** aus.
4. Ändern Sie den Gerätenamen im entsprechenden Feld und klicken Sie danach auf **Speichern**.

Falls der Autopilot deaktiviert wurde, können Sie ihn mit einem Klick auf den Schalter wieder aktivieren. Klicken Sie **Speichern**, um die Einstellungen zu speichern.

Sie können für jedes Ihrer Geräte zur einfacheren Verwaltung einen Besitzer anlegen und zuordnen:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf das ⋮ -Symbol auf der gewünschten Gerätekarte und wählen Sie **Profil** aus.

4. Kicken Sie auf **Besitzer hinzufügen**, füllen Sie die entsprechenden Felder aus, geben Sie Geschlecht und Geburtsdatum ein und fügen Sie bei Bedarf ein Profilbild hinzu.
5. Klicken Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
6. Wählen Sie aus der **Gerätebesitzer**-Liste den gewünschten Besitzer aus und klicken Sie auf **ZUORDNEN**.

So können Sie Bitdefender per Fernzugriff auf Ihren Geräten aktualisieren:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf das ⋮ -Symbol auf der gewünschten Gerätekarte und wählen Sie **Update** aus.

Klicken Sie auf die entsprechende Gerätekarte, um das Gerät per Fernzugriff zu steuern oder Informationen zu Ihrem Bitdefender-Produkt auf einem bestimmten Geräte anzuzeigen.

Klicken Sie auf eine Gerätekarte, um die folgenden Reiter anzuzeigen:

- **Dashboard** . In diesem Fenster können Sie den Sicherheitsstatus Ihrer Bitdefender-Produkte sowie die verbleibende Dauer Ihres Abonnements einsehen. Der Sicherheitsstatus Ihres Produktes ist entweder grün - es sind keine Probleme aufgetreten - oder rot, in diesem Falle ist Ihr Gerät gefährdet. Falls bei Ihrem Produkt Probleme aufgetreten sind, können Sie mit einem Klick auf **Probleme anzeigen** weitere Details abrufen. Von hier aus können die Probleme, die Ihre Gerätesicherheit beeinträchtigen, manuell behoben werden.
- **Schutz**. Über dieses Fenster können Sie per Fernzugriff einen Quick Scan oder eine Systemprüfung veranlassen. Klicken Sie auf **SCAN**, um den Vorgang zu starten. Sie können auch nachvollziehen, wann der letzte Scan auf dem Gerät durchgeführt wurde, und einen Bericht für den aktuellsten Scan abrufen, in dem die wichtigsten Informationen zusammengefasst werden.Weitere Informationen zu diesen Scan-Optionen finden Sie in den Kapiteln *„Durchführen von System-Scans“* (S. 86) und *„Durchführen von Quick Scans“* (S. 86).
- **Schwachstelle**. Über die **SCAN**-Schaltfläche im Reiter Schwachstellen können Sie ein Gerät auf Schwachstellen, fehlende Windows-Updates, veraltete Anwendungen oder unsichere Passwörter überprüfen.

Schwachstellen können nicht per Fernzugriff behoben werden. Falls eine Schwachstelle gefunden wird, müssen Sie den Schwachstellen-Scan mit dem jeweiligen Gerät wiederholen und die vorgeschlagenen Maßnahmen ergreifen. Weitere Informationen zu dieser Funktion finden Sie im Kapitel *„Schwachstellen“* (S. 110).

7. BITDEFENDER AUF DEM NEUESTEN STAND HALTEN

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm Bitdefender stets mit den neuesten Virensignaturen betreiben.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet Bitdefender eigenständig. Standardmäßig sucht die Software nach Updates, wenn Sie Ihren Computer einschalten und danach einmal pro **Stunde**. Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.

Der Updatevorgang wird "on the fly" durchgeführt. Das bedeutet, dass die entsprechenden Dateien stufenweise aktualisiert werden. So stört der Update-Vorgang nicht den Betrieb des Produkts, während gleichzeitig alle Schwachstellen behoben werden.

Wichtig
Um immer vor den neuesten Bedrohungen geschützt zu sein, sollte das automatische Update immer aktiviert bleiben.

In manchen Situationen kann es notwendig werden, dass Sie eingreifen, um den Bitdefender-Schutz auf dem neuesten Stand zu halten:

- Wenn Ihr Computer über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen wie unter *„Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?“* (S. 72) beschrieben konfigurieren.
- Wenn Sie über keine Internet-Verbindung verfügen, können Sie Bitdefender, wie im Kapitel *„Mein Computer ist nicht mit dem Internet verbunden. Wie kann ich Bitdefender aktualisieren?“* (S. 148) beschrieben, auch manuell aktualisieren. Die Datei für das manuelle Update wird einmal pro Woche veröffentlicht.
- Bei einer langsamen Internetverbindung können Fehler beim Herunterladen von Updates auftreten. Um zu erfahren, wie Sie solche Fehlern vermeiden können, lesen Sie bitte das Kapitel *„Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann“* (S. 147).

- Falls Sie sich per Einwahl mit dem Internet verbinden, ist es sinnvoll, regelmäßig ein manuelles Bitdefender-Update durchzuführen. Für weitere Informationen lesen Sie bitte *„Durchführung eines Updates“ (S. 47)*.

7.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist

Links in der Symbolleiste wird im **Sicherheitstatusbereich** der Zeitpunkt des letzten Bitdefender-Updates angezeigt.

Um ausführliche Informationen zu Ihren letzten Updates zu erhalten, rufen Sie die Update-Ereignisse auf:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
2. Wählen Sie im Fenster **Ereignisanzeige Update** aus dem entsprechenden Menü aus.

Sie können herausfinden, wann Updates angestoßen wurden und weitere Informationen dazu einholen (d.h. ob sie erfolgreich waren oder nicht, ob ein Neustart erforderlich ist, um die Installation abzuschließen). Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

7.2. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

Sie haben folgende Möglichkeiten, ein Update zu starten:

- Öffnen Sie die Bitdefender-Benutzeroberfläche und klicken Sie auf die **Update**-Schaltfläche.
- Rechtsklicken Sie in der Task-Leiste auf das -Bitdefender-Symbol und wählen Sie **Jetzt aktualisieren**.

Das Update-Modul verbindet sich mit dem Bitdefender-Update-Server und sucht nach verfügbaren Updates. Wenn ein Update erkannt wird, werden Sie abhängig von den Update-Einstellungen entweder aufgefordert, dies zu bestätigen oder das Update wird automatisch durchgeführt.

Wichtig

Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen, das so bald wie möglich zu tun.

Sie können die Updates auf Ihren Geräten zudem per Fernzugriff vornehmen, vorausgesetzt, sie sind eingeschaltet und mit dem Internet verbunden.

So können Sie Bitdefender per Fernzugriff auf Ihren Geräten aktualisieren:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf das -Symbol auf der gewünschten Gerätekarte und wählen Sie **Update** aus.

7.3. Aktivieren / Deaktivieren der automatischen Updates

Um das automatische Update zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Update** aus.
3. Klicken Sie auf den Schalter, um automatische Updates zu aktivieren oder deaktivieren.
4. Ein Warnung wird angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange die automatischen Updates deaktiviert bleiben sollen. Sie können automatische Updates für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren.

Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen, die automatischen Updates so kurz wie möglich zu deaktivieren. Denn Bitdefender kann Sie nur dann gegen die neusten Bedrohungen schützen, wenn es auf dem neuesten Stand ist.

7.4. Update-Einstellungen anpassen

Updates können im lokalen Netzwerk, über das Internet, direkt oder durch einen Proxy-Server durchgeführt werden. Standardmäßig scannt Bitdefender jede Stunde auf neue Updates und installiert diese ohne Ihr Zutun.

Die standardmäßigen Update-Einstellungen eignen sich für die meisten Benutzer und es ist normalerweise nicht erforderlich, diese zu ändern.

Um die Update-Einstellungen anzupassen, gehen Sie folgendermaßen vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Update** aus und passen Sie die Einstellungen Ihren Anforderungen an.

Update-Häufigkeit

Bitdefender ist für eine stündliche Update-Prüfung konfiguriert. Die Update-Häufigkeit lässt sich durch Schieben des entsprechenden Reglers auf den gewünschten Update-Zeitraum festlegen.

Update-Server

Bitdefender ist so konfiguriert, dass Updates von den Bitdefender-Update-Servern aus dem Internet heruntergeladen werden. Die Update-Adresse ist eine generische Internetadresse, die automatisch zu dem Bitdefender-Update-Server, der sich am nächsten zu Ihrem Standort befindet, umgeleitet wird.

Verändern Sie die Update-Adresse nicht, es sei denn, Sie werden von einem Bitdefender-Mitarbeiter oder Ihrem Netzwerkadministrator (falls Sie mit einem Unternehmensnetzwerk verbunden sind) ausdrücklich dazu aufgefordert.

Klicken Sie auf **Standard**, um die ursprüngliche Update-Adresse wiederherzustellen.

Update-Verarbeitungsregeln

Es gibt drei Möglichkeiten, Updates herunterzuladen und zu installieren:

- **Update im Hintergrund** - Bitdefender Updates werden automatisch heruntergeladen und installiert.
- **Vor dem Download nachfragen** - Sobald ein Update verfügbar ist, werden Sie gefragt, ob es heruntergeladen werden soll.
- **Vor der Installation nachfragen** - Sobald ein Update heruntergeladen wurde, werden Sie gefragt, ob die Installation durchgeführt werden soll.

Manche Updates erfordern einen Neustart, um die Installation abzuschließen. Sollte ein Update einen Neustart erforderlich machen, arbeitet Bitdefender standardmäßig mit den alten Dateien weiter, bis der Benutzer den Computer aus eigenen Stücken neu startet. Dadurch soll verhindert werden, dass der Update-Prozess von Bitdefender den Benutzer in seiner Arbeit behindert.

Wenn Sie eine Meldung erhalten möchten, sobald ein Update einen Neustart erfordert, deaktivieren Sie die Option **Neustart verschieben**, indem Sie auf den entsprechenden Schalter klicken.

GEWUSST WIE

8. INSTALLATION

8.1. Wie installiere ich Bitdefender auf einem zweiten Computer?

Falls Ihr Abonnement für mehrere Geräte gültig ist, können Sie Ihre Bitdefender Central-Anmeldedaten verwenden, um einen zweiten PC zu registrieren.

So installieren Sie Bitdefender auf einem zweiten Computer:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie im Fenster **Meine Geräte** auf **Bitdefender installieren**.
4. Wählen Sie zunächst **Windows** und danach eine der beiden Optionen aus:
   - Ich möchte Bitdefender **Auf diesem Gerät** installieren.

     Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus und klicken Sie auf **Herunterladen**, um fortzufahren.
   - Ich möchte Bitdefender **Auf einem anderen Gerät** installieren.

     Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.
5. Führen Sie das von Ihnen heruntergeladene Bitdefender aus. Warten Sie, bis die Registrierung abgeschlossen ist und schließen Sie dann das Fenster.

Das neue Gerät, auf dem Sie das Bitdefender-Produkt installiert haben, wird ab sofort im Bitdefender Central-Dashboard angezeigt.

8.2. Wann sollte ich Bitdefender neu installieren?

Es gibt Situationen, die es erforderlich machen könnten, dass Sie Ihr Bitdefender-Produkt erneut installieren.

Die Folgenden sind typische Situationen, in denen Sie Bitdefender erneut installieren müssen:

- Sie haben das Betriebssystem neu installiert..

- Sie haben einen neuen Computer erworben..
- Sie wollen die Anzeigesprache der Bitdefender-Benutzeroberfläche ändern..

Um Bitdefender neu zu installieren, können Sie den von Ihnen erworbenen Installationsdatenträger verwenden oder eine neue Version über Ihr Bitdefender Central-Benutzerkonto herunterladen.

Weitere Information zum Bitdefender-Installationsprozess finden Sie im Kapitel *„Installieren Ihres Bitdefender-Produkts“* (S. 5).

8.3. Wo kann ich mein Bitdefender-Produkt herunterladen?

Sie können Bitdefender vom Installationsdatenträger installieren oder den Web-Installer verwenden, der über die Bitdefender Central-Plattform heruntergeladen werden kann.

Beachten Sie

Bevor Sie das Installationspaket ausführen, sollten Sie jede andere auf Ihrem System installierte Virenschutzlösung entfernen. Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Computer verwenden, wird dadurch das System instabil.

So können Sie Bitdefender über Ihr Bitdefender Central-Benutzerkonto installieren:

1. Rufen Sie Ihr Bitdefender Central-Konto auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie im Fenster **Meine Geräte** auf **Bitdefender installieren**.
4. Wählen Sie zunächst **Windows** und danach eine der beiden Optionen aus:
   - Ich möchte Bitdefender **Auf diesem Gerät** installieren.

     Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus und klicken Sie auf **Herunterladen**, um fortzufahren.
   - Ich möchte Bitdefender **Auf einem anderen Gerät** installieren.

     Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.
5. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.

8.4. Wie verfahre ich mit meinem Bitdefender-Abonnement nach einem Windows-Upgrade?

Diese Situation tritt ein, wenn Sie Ihr Betriebssystem aktualisieren und Sie Ihren Bitdefender-Abonnement weiterhin nutzen möchten.

Sollten Sie eine vorausgegangene Bitdefender-Version nutzen, können Sie ein kostenloses Upgrade auf die neueste Version von Bitdefender wie folgt durchführen:

- Von einer Vorgängerversion von Bitdefender Antivirus auf die aktuelle Version von Bitdefender Antivirus.
- Von einer Vorgängerversion von Bitdefender Internet Security auf die aktuelle Version von Bitdefender Internet Security.
- Von einer Vorgängerversion von Bitdefender Total Security auf die aktuelle Version von Bitdefender Total Security.

Hierbei gibt es 2 Szenarien:

- Sie haben Ihr Betriebssystem über Windows Update aktualisiert und bemerken, dass Bitdefender nicht mehr funktioniert.

  In diesem Fall müssen Sie das Produkt in der aktuellsten Version erneut installieren.

  Gehen Sie dabei folgendermaßen vor:

  1. Entfernen Sie Bitdefender, indem Sie wie folgt vorgehen:
     - In **Windows 7**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
       b. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
       c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
       d. Klicken Sie auf **Weiter**.
       e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 8 und Windows 8.1**:
  a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  c. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
  d. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
  e. Klicken Sie auf **Weiter**.
  f. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
- In **Windows 10**:
  a. Klicken Sie auf **Start** und danach auf Einstellungen.
  b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
  c. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
  d. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
  e. Klicken Sie auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren**.
  f. Klicken Sie auf **Weiter**.
  g. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

2. Laden Sie die Installationsdatei herunter:
   a. Rufen Sie Ihr Bitdefender Central-Konto auf.
   b. Rufen Sie den Bereich **Meine Geräte** auf.
   c. Klicken Sie im Fenster **Meine Geräte** auf **Bitdefender installieren**.
   d. Wählen Sie zunächst **Windows** und danach eine der beiden Optionen aus:

- Ich möchte Bitdefender **Auf diesem Gerät** installieren.

  Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus und klicken Sie auf **Herunterladen**, um fortzufahren.

- Ich möchte Bitdefender **Auf einem anderen Gerät** installieren.

  Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.

3. Öffnen Sie den Ordner mit dem Installationsprogramm und führen Sie es per Doppelklick aus, um den Installationsvorgang zu starten.

- Sie haben Ihr System gewechselt und möchten nicht auf den Bitdefender-Schutz verzichten.

  Deshalb müssen Sie das Produkt in der aktuellsten Version erneut installieren.

  Verfahren Sie in einer solchen Situation wie folgt:

  1. Laden Sie die Installationsdatei herunter:
     a. Rufen Sie Ihr Bitdefender Central-Konto auf.
     b. Rufen Sie den Bereich **Meine Geräte** auf.
     c. Klicken Sie im Fenster **Meine Geräte** auf **Bitdefender installieren**.
     d. Wählen Sie zunächst **Windows** und danach eine der beiden Optionen aus:
        - Ich möchte Bitdefender **Auf diesem Gerät** installieren.

          Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus und klicken Sie auf **Herunterladen**, um fortzufahren.

        - Ich möchte Bitdefender **Auf einem anderen Gerät** installieren.

          Wählen Sie unter **Zu installierendes Produkt** Bitdefender Antivirus Plus 2016 aus. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.

  2. Öffnen Sie den Ordner mit dem Installationsprogramm und führen Sie es per Doppelklick aus, um den Installationsvorgang zu starten.

  Weitere Information zum Bitdefender-Installationsprozess finden Sie im Kapitel *„Installieren Ihres Bitdefender-Produkts“* (S. 5).

8.5. Wie kann ich Bitdefender reparieren?

Um Ihr Bitdefender Antivirus Plus 2016 über das Windows-Startmenü zu reparieren, gehen Sie folgendermaßen vor:

- In **Windows 7**:
  1. Klicken Sie auf **Start** und **Alle Programme**.
  2. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
  3. Klicken Sie im angezeigten Fenster auf **Reparieren**.

     Dies kann einige Minuten in Anspruch nehmen.
  4. Sie müssen den Computern neu starten, um den Vorgang abzuschließen.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
  4. Klicken Sie im angezeigten Fenster auf **Reparieren**.

     Dies kann einige Minuten in Anspruch nehmen.
  5. Sie müssen den Computern neu starten, um den Vorgang abzuschließen.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie **Apps & Funktionen** aus.
  3. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
  5. Klicken Sie auf **Reparieren**.

     Dies kann einige Minuten in Anspruch nehmen.
  6. Sie müssen den Computern neu starten, um den Vorgang abzuschließen.

9. ABONNEMENTS

9.1. Welches Bitdefender-Produkt nutze ich?

So ermitteln Sie, welches Bitdefender-Programm auf Ihrem Gerät installiert ist:

1. Öffnen Sie das Bitdefender-Hauptfenster.
2. Am oberen Rand des Fensters sollten Sie einen der folgenden Schriftzüge sehen:
   - Bitdefender Antivirus Plus 2016
   - Bitdefender Internet Security 2016
   - Bitdefender Total Security 2016

9.2. Wie kann ich mein Bitdefender-Abonnement mithilfe eines Lizenzschlüssels aktivieren?

Es gibt zwei Möglichkeiten, einen gültigen Lizenzschlüssel zur Aktivierung eines Bitdefender Antivirus Plus 2016-Abonnements zu verwenden:

- Im Falle eines Upgrades auf die neueste Bitdefender-Version:
  1. Nach Abschluss des Bitdefender Antivirus Plus 2016-Upgrades werden Sie aufgefordert, sich bei Ihrem Bitdefender Central-Konto anzumelden.
  2. Geben Sie Ihre Anmeldedaten ein und klicken Sie auf **EINLOGGEN**.
  3. In Ihrem Benutzerkonto wird eine Meldung angezeigt, die die Anlage des Abonnements bestätigt. Das neu angelegte Abonnement ist für die verbleibende Gültigkeitsdauer Ihres Lizenzschlüssels und für die gleiche Anzahl an Benutzern gültig.

     Auf allen Geräten, die noch alte Bitdefender-Versionen nutzen und die mit dem Lizenzschlüssel registriert wurden, der nun in ein Abonnement umgewandelt wurde, muss das Produkt mit dem gleichen Bitdefender Central-Konto registriert werden.
- Im Falle, dass Bitdefender bisher noch nicht auf dem System installiert war:
  1. Nach Abschluss des Installationsvorgangs werden Sie aufgefordert, sich bei Ihrem Bitdefender Central-Konto anzumelden.

2. Geben Sie Ihre Anmeldedaten ein und klicken Sie auf **EINLOGGEN**.
3. Rufen Sie den Bereich **Meine Abonnements** auf.
4. Klicken Sie auf **Lizenzschlüssel hinzufügen** und geben Sie Ihren Lizenzschlüssel ein.
5. Ein Abonnement mit der gleichen Gültigkeitsdauer und Anzahl an Benutzern wie Ihr Lizenzschlüssel wird mit Ihrem Benutzerkonto verknüpft.

10. BITDEFENDER CENTRAL

10.1. Wie melde ich mit einem anderen Benutzerkonto bei Bitdefender Central an?

Sie haben ein neues Bitdefender Central-Konto angelegt und möchten es von nun an nutzen.

Um ein anderes Benutzerkonto nutzen zu können, gehen Sie folgendermaßen vor:

1. Klicken Sie oben im Bitdefender-Fenster auf das -Symbol und wählen Sie **Kontodetails** aus dem Menü aus.
2. Klicken Sie auf **Konto wechseln**, um den Computer mit einem anderen Benutzerkonto zu verknüpfen.
3. Geben Sie die E-Mail-Adresse und das Kennwort Ihres Kontos in die entsprechenden Felder ein und klicken Sie auf **EINLOGGEN**.

Beachten Sie

Das Bitdefender-Produkt auf Ihrem Gerät wird entsprechend dem mit Ihrem neuen Bitdefender Central-Konto verknüpften Abonnement automatisch umgestellt.
Falls mit dem neuen Bitdefender Central-Konto kein verfügbares Abonnement verknüpft ist oder Sie es von einem früheren Benutzerkonto übernehmen möchten, können Sie sich wie in Kapitel *„Hilfe anfordern“* (S. 166) beschrieben mit dem Bitdefender-Support in Verbindung setzen.

10.2. Wie setzte ich das Passwort für mein Bitdefender Central-Konto zurück?

Um ein neues Passwort für Ihr Bitdefender Central-Konto festzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie oben im Bitdefender-Fenster auf das -Symbol und wählen Sie **Kontodetails** aus dem Menü aus.
2. Klicken Sie auf **Konto wechseln**, um den Computer mit einem anderen Benutzerkonto zu verknüpfen.

   Ein neues Fenster wird angezeigt.

3. Klicken Sie auf den **Zurücksetzen des Passworts**-Link.
4. Geben Sie die E-Mail-Adresse ein, mit der Sie Ihr Bitdefender Central-Konto angelegt haben, und klicken Sie auf **PASSWORT ZURÜCKSETZEN**.
5. Rufen Sie Ihre E-Mails ab und klicken Sie auf den entsprechenden Link.
6. Geben Sie Ihre E-Mail-Adresse in das entsprechende Feld ein.
7. Geben Sie das neue Passwort ein. Das Passwort muss mindestens 8 Zeichen lang sein und Zahlen enthalten.
8. Klicken Sie auf **PASSWORT FESTLEGEN**.

Geben Sie von jetzt an Ihre E-Mail-Adresse und das neue Passwort ein, um auf Ihr Bitdefender Central-Konto zuzugreifen.

11. PRÜFEN MIT BITDEFENDER

11.1. Wie kann ich eine Datei oder einen Ordner scannen?

Um eine Datei oder einen Ordner einfach und schnell zu scannen, klicken Sie mit der rechten Maustaste auf das Objekt, das Sie scannen möchten, wählen Sie Bitdefender und anschließend **Mit Bitdefender scannen** aus dem Menü.

Um den Scan abzuschließen, folgen Sie den Anweisungen des Scan-Assistenten. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Typische Situationen, für die diese Scan-Methode geeignet ist:

- Sie vermuten, dass eine bestimmte Datei oder ein Ordner infiziert ist.
- Immer dann, wenn Sie aus dem Internet Dateien herunterladen, von deren Ungefährlichkeit Sie nicht überzeugt sind.
- Scannen Sie einen freigegebenen Ordner, bevor Sie die enthaltenen Dateien auf Ihren Rechner kopieren.

11.2. Wie scanne ich mein System?

Um einen vollständigen System-Scan durchzuführen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Wählen Sie im Modul **Virenschutz System-Scan** aus.
4. Folgen Sie den Anweisungen des Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.

   Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Für weitere Informationen lesen Sie bitte *„Viren-Scan-Assistent“ (S. 91)*.

11.3. Wie plane ich einen Scan?

Sie können Ihr Bitdefender-Produkt so konfigurieren, dass es wichtige Systembereiche nur dann scannt, wenn Sie Ihren Computer nicht benötigen.

So legen Sie einen Zeitplan für einen Scan fest:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Wählen Sie im Modul **Virenschutz Scans verwalten** aus.
4. Wählen Sie den Scan-Typ aus, für den Sie einen Zeitplan festlegen möchten - System-Scan oder Quick Scan - und klicken Sie danach auf **Scan-Optionen**.

   Alternativ können Sie mit einem Klick auf **Neue benutzerdefinierte Aufgabe** einen eigenen Scan-Typ nach Ihren Anforderungen anlegen.
5. Aktivieren Sie den Schalter **Planen**.

   Wählen Sie eine der entsprechenden Optionen, um einen Zeitplan festzulegen:

   - Start bei Systemneustart
   - Einmal
   - Periodisch

Im Fenster **Scan-Ziele** können Sie die Systembereiche festlegen, die gescannt werden sollen.

11.4. Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen?

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierte Scan-Aufgabe konfigurieren und ausführen.

Um eine benutzerdefinierte Scan-Aufgabe anzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Wählen Sie im Modul **Virenschutz Scans verwalten** aus.
4. Klicken Sie auf **Neue benutzerdefinierte Aufgabe**. Klicken Sie auf den Reiter **Basic**, um einen Namen für den Scan einzugeben und die Bereiche auszuwählen, die gescannt werden sollen.
5. Um die Scan-Optionen im Detail zu konfigurieren, wählen Sie den Reiter **Erweitert**.

   Sie können die Scan-Optionen einfach durch Einstellen der Scan-Tiefe festlegen. Schieben Sie den Regler dazu in die gewünschte Position.

   Sie können auch festlegen, dass der Computer heruntergefahren wird, wenn der Scan beendet und keine Bedrohung erkannt wurde. Bitte beachten Sie, dass dies das Standardverhalten bei jeder Ausführung dieser Aufgabe sein wird.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
7. Klicken Sie auf den entsprechenden Schalter, um einen Zeitplan für Ihre Scan-Aufgabe festzulegen.
8. Klicken Sie auf **Scan starten** und folgen Sie den Anweisungen des Scan-Assistenten, um den Scan abzuschließen. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.
9. Bei Bedarf können Sie einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste klicken.

11.5. Wie kann ich einen Ordner vom Scan ausnehmen?

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausschließen.

Ausschlüsse sollten nur von Benutzern eingesetzt werden, die erfahren im Umgang mit Computern sind und nur in den folgenden Situationen:

- Sie haben einen großen Ordner mit Filmen und Musik auf Ihrem System gespeichert.
- Sie haben ein großes Archiv mit verschiedenen Daten auf Ihrem System gespeichert.
- Sie haben einen Ordner, in dem Sie verschiedene Software-Typen und Anwendungen zu Testzwecken installieren. Ein Scan des Ordners könnte zum Verlust einiger der Daten führen.

Um den Ordner des Ausschlussliste hinzuzufügen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Ausschlüsse**.
4. Vergewissern Sie sich, dass der Schalter für **Ausschlüsse für Dateien** auf EIN steht.
5. Klicken Sie auf den Link **Ausgeschlossene Dateien und Ordner**.
6. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
7. Klicken Sie auf **Durchsuchen**, wählen Sie den Ordner, der vom Scan ausgeschlossen werden soll, und klicken Sie auf **OK**.
8. Klicken Sie auf **Hinzufügen** und danach auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

11.6. Wie gehe ich vor, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat?

Es können Situationen auftreten, in denen Bitdefender einwandfreie Dateien irrtümlicherweise als Bedrohung einstuft (Fehlalarm). Um diesen Fehler zu korrigieren, fügen Sie die Datei der Bitdefender-Ausschlussliste hinzu:

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:

a. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.

b. Wechseln Sie zum Reiter **Schutz**.

c. Klicken Sie auf das Modul **Virenschutz**.

d. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.

e. Klicken Sie auf den Schalter, um **Zugriff-Scan** zu deaktivieren.

Ein Warnung wird angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Sie können den Echtzeitschutz für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren.

2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 74).

3. Stellen Sie die Datei aus der Quarantäne wieder her:

a. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.

b. Wechseln Sie zum Reiter **Schutz**.

c. Klicken Sie im Modul **Virenschutz** auf den Reiter **Quarantäne**.

d. Wählen Sie die Datei aus und klicken Sie auf **Wiederherstellen**.

4. Fügen Sie die Datei zur Ausschlussliste hinzu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie kann ich einen Ordner vom Scan ausnehmen?“* (S. 64).

5. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

6. Setzten Sie sich mit unseren Support-Mitarbeitern in Verbindung, damit wir die Erkennungssignatur entfernen können. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Hilfe anfordern“* (S. 166).

11.7. Wo sehe ich, welche Viren Bitdefender gefunden hat?

Nach jedem durchgeführten Scan wird ein Protokoll erstellt, in dem Bitdefender alle gefundenen Probleme aufzeichnet.

Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **Protokoll anzeigen** klicken.

Wenn Sie ein Scan-Protokoll lesen oder eine gefundene Infektion einsehen möchten, gehen Sie dazu wie folgt vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
2. Wählen Sie im Fenster **Ereignisanzeige** **Virenschutz** aus dem entsprechenden Menü aus.

   Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.
3. In der Ereignisliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
4. Um ein Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**.

   Klicken Sie auf **Erneut scannen**, um einen Scan zu wiederholen.

12. PRIVATSPHÄRENSCHUTZ

12.1. Wie sichere ich meine Online-Transaktionen ab?

Um Ihre Online-Transaktionen wie Online-Banking noch sicherer zu machen, können Sie den Browser von Bitdefender verwenden.

Bitdefender Safepay™ ist ein abgesicherter Browser, der Ihre Kreditkartennummern, Kontonummern und andere sensible Daten, die Sie bei Online-Transaktionen eingeben, zuverlässig schützt.

So sichern Sie Ihre Online-Transaktionen ab:

1. Klicken Sie im Bitdefender-Hauptfenster auf die **Safepay**-Schaltfläche.
2. Klicken Sie auf die Schaltfläche , um die **Virtuelle Tastatur** aufzurufen.
3. Verwenden Sie die **Virtuelle Tastatur** immer dann, wenn Sie sensible Informationen wie Passwörter eingeben.

12.2. Wie lösche ich mit Bitdefender eine Datei unwiderruflich?

Wenn Sie eine Datei unwiderruflich von Ihrem System löschen möchten, müssen Sie die Datei physisch von Ihrer Festplatte entfernen.

Mit dem Bitdefender-Dateischredder können Sie über das Windows-Kontextmenü Dateien oder Ordner auf Ihrem Computer schnell und einfach schreddern. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, den Sie unwiderruflich löschen möchten, wählen Sie Bitdefender und anschließend **Dateischredder**.
2. Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **Ja**, um den Assistenten für den Dateischredder zu starten.
3. Bitte warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.
4. Die Ergebnisse werden angezeigt. Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

13. NÜTZLICHE INFORMATIONEN

13.1. Wie teste ich meine Virenschutzlösung?

Um die ordnungsgemäße Funktion Ihres Bitdefender-Produkts zu überprüfen, empfehlen wir den EICAR-Test.

Dabei testen Sie mithilfe der speziell für diesen Zweck entwickelten EICAR-Testdatei Ihren Virenschutz.

Um Ihre Virenschutzlösung zu testen, gehen Sie folgendermaßen vor:

1. Laden Sie die Testdatei von der offiziellen EICAR-Website unter http://www.eicar.org/ herunter.
2. Klicken Sie auf den Reiter **Anti-Malware Testfile**.
3. Klicken Sie im Menü links auf **Download**.
4. Klicken Sie unter **Download area using the standard protocol http** auf die **eicar.com**-Testdatei.
5. Sie werden informiert, dass die von Ihnen aufgerufene Seite die EICAR-Testdatei (kein Virus) enthält.

   Wenn Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken, beginnt der Download der Testdatei und ein Bitdefender-Fenster informiert Sie, dass ein Virus erkannt wurde.

   Klicken Sie auf **Mehr...** für weitere Informationen.

Falls Sie keine Bitdefender-Benachrichtigung erhalten, empfehlen wir Ihnen, sich wie in Kapitel *„Hilfe anfordern“ (S. 166)* beschrieben an Bitdefender zu wenden.

13.2. Wie kann ich Bitdefender entfernen?

Um Ihr Bitdefender Antivirus Plus 2016 zu entfernen, gehen Sie folgendermaßen vor:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.

3. Wählen Sie zunächst **Entfernen** und danach **Ich möchte es dauerhaft entfernen** aus.
4. Klicken Sie auf **Weiter**.
5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 8 und Windows 8.1**:

1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
3. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
4. Wählen Sie zunächst **Entfernen** und danach **Ich möchte es dauerhaft entfernen** aus.
5. Klicken Sie auf **Weiter**.
6. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 10**:

1. Klicken Sie auf **Start** und danach auf Einstellungen.
2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
3. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
5. Wählen Sie zunächst **Entfernen** und danach **Ich möchte es dauerhaft entfernen** aus.
6. Klicken Sie auf **Weiter**.
7. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

13.3. Wie fahre ich den Computer automatisch herunter, nachdem der Scan beendet wurde?

Bitdefender bietet unterschiedliche Scan-Aufgaben, mithilfe derer Sie sicherstellen können, dass Ihr System nicht mit Malware infiziert ist. Je nach Software- und Hardwarekonfiguration kann ein Scan des gesamten Systems längere Zeit in Anspruch nehmen.

Deshalb können Sie Bitdefender so konfigurieren, dass Bitdefender den Computer herunterfährt, sobald der Scan abgeschlossen ist.

Stellen Sie sich folgende Situation vor: Sie sind mit der Arbeit an Ihrem Computer fertig und möchten ins Bett gehen. Sie möchten aber nun noch Ihr System durch Bitdefender auf Malware prüfen lassen.

So können Sie einstellen, dass Bitdefender den Computer herunterfährt, sobald der Scan abgeschlossen ist:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Wählen Sie im Modul **Virenschutz Scans verwalten** aus.
4. Klicken Sie im Fenster **Scan-Aufgaben verwalten** auf **Neue benutzerdefinierte Aufgabe**, um einen Namen für den Scan einzugeben und die Bereiche auszuwählen, die gescannt werden sollen.
5. Um die Scan-Optionen im Detail zu konfigurieren, wählen Sie den Reiter **Erweitert**.
6. Markieren Sie die Option, dass der Computer heruntergefahren wird, wenn der Scan beendet und keine Bedrohung gefunden wurde.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
8. Klicken Sie auf **Scan starten**, um Ihr System zu scannen.

Wenn keine Bedrohungen gefunden wurden, wird der Computer heruntergefahren.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Für weitere Informationen lesen Sie bitte *„Viren-Scan-Assistent“* (S. 91).

13.4. Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?

Wenn Ihr Computer sich über einen Proxy-Server mit dem Internet verbindet, müssen Sie Bitdefender mit den Proxy-Einstellungen konfigurieren. Normalerweise findet und importiert Bitdefender automatisch die Proxy-Einstellungen Ihres Systems.

Wichtig
Internet-Verbindungen in Privathaushalten nutzen üblicherweise keine Proxy-Server. Als Faustregel gilt, dass Sie die Einstellungen der Proxy-Verbindung Ihrer Bitdefender-Anwendung prüfen und konfigurieren sollten, falls Updates nicht funktionieren. Wenn Bitdefender sich aktualisieren kann, dann ist es richtig konfiguriert, um eine Verbindung mit dem Internet aufzubauen.

Um die Proxy-Einstellungen zu verwalten, gehen Sie folgendermaßen vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Erweitert** aus.
3. Klicken Sie auf den Schalter, um die Proxy-Nutzung einzuschalten.
4. Klicken Sie auf den Link **Proxyverwaltung**
5. Sie haben zwei Möglichkeiten, die Proxy-Einstellungen vorzunehmen:
   - **Proxy-Einstellungen aus Standard-Browser importieren** - Proxy-Einstellungen des aktuellen Benutzers, aus dem Standard-Browser importiert. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.

     Beachten Sie
     Bitdefender kann die Proxy-Einstellungen aus den gängigsten Browsern importieren, einschließlich der neuesten Versionen von Internet Explorer, Mozilla Firefox und Opera.

   - **Benutzerdefinierte Proxy-Einstellungen** - Proxy-Einstellungen, die Sie selbst konfigurieren können. Die folgenden Einstellungen müssen angegeben werden:
     - **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.

- **Port** - Geben Sie den Port ein, über den Bitdefender die Verbindung zum Proxy-Server herstellt.
- **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
- **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.

6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Bitdefender wird die verfügbaren Proxy-Einstellungen verwenden, bis die Lösung eine Verbindung mit dem Internet aufbauen kann.

13.5. Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?

Um herauszufinden, ob auf Ihrem Computer ein 32- oder 64-Bit-Betriebssystem installiert ist, gehen Sie wie folgt vor:

- In **Windows 7**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Computer** im **Start**-Menü.
  3. Rechtsklicken Sie auf **Arbeitsplatz** und wählen Sie **Eigenschaften**.
  4. Unter **System** können Sie die Systeminformationen einsehen.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite den Eintrag **Computer** (z.B. durch die Eingabe von "Computer" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Wählen Sie im Menü unten **Eigenschaften**.
  3. Im Bereich System finden Sie Ihren Systemtyp.
- In **Windows 10**:
  1. Geben Sie "System" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
  2. Im Bereich System finden Sie Informationen zu Ihrem Systemtyp.

13.6. Wie kann ich in Windows versteckte Objekte anzeigen?

Diese Schritte sind sinnvoll in den Fällen, in denen Sie es mit einer Malware-Situation zu tun haben und Sie infizierte Dateien, die eventuell verborgen sind, finden und entfernen müssen.

Gehen Sie folgendermaßen vor, um versteckte Objekte in Windows anzuzeigen:

1. Klicken Sie auf **Start** und öffnen Sie die **Systemsteuerung**.

   In **Windows 8 und Windows 8.1**: Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

2. Klicken Sie auf **Ordneroptionen**.
3. Gehen Sie auf den Reiter **Ansicht**.
4. Wählen Sie **Verborgene Dateien und Verzeichnisse anzeigen**.
5. Entfernen Sie den Haken bei **Erweiterungen bei bekannten Dateitypen ausblenden**.
6. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
7. Klicken Sie auf **Anwenden** und danach auf **OK**.

In **Windows 10**:

1. Geben Sie "Alle Dateien und Ordner anzeigen" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
2. Wählen Sie **Ausgeblendete Dateien, Ordner und Laufwerke anzeigen** aus.
3. Entfernen Sie den Haken bei **Erweiterungen bei bekannten Dateitypen ausblenden**.
4. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
5. Klicken Sie auf **Anwenden** und danach auf **OK**.

13.7. Wie entferne ich andere Sicherheitslösungen?

Der Hauptgrund für den Einsatz einer Sicherheitslösung ist der Schutz und die Sicherheit Ihrer Daten. Aber was geschieht, wenn mehr als ein Sicherheitsprogramm auf demselben System läuft?

Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Computer verwenden, wird dadurch das System instabil. Das Bitdefender Antivirus Plus 2016-Installationsprogramm findet automatisch andere auf dem System installierte Sicherheits-Software und bietet an, diese zu deinstallieren.

Falls Sie weitere bereits auf dem PC installierte Sicherheits-Software nicht während der Installation entfernt haben, gehen Sie folgendermaßen vor:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  4. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

Wenn es Ihnen nicht gelingt, weitere auf Ihrem Rechner installierte Sicherheits-Software zu entfernen, laden Sie sich das Deinstallations-Tool von der Website des entsprechenden Herstellers herunter oder wenden Sie sich direkt an den Hersteller für eine Deinstallationsanleitung.

13.8. Wie führe ich einen Neustart im abgesicherten Modus durch?

Der abgesicherte Modus ist ein diagnostischer Betriebsmodus, der hauptsächlich bei der Suche nach Fehlern zum Einsatz kommt, die den normalen Windows-Betrieb beeinträchtigen. Solche Probleme reichen von in Konflikt stehenden Treibern bis hin zu Viren, die Windows daran hindern, normal hochzufahren. Im abgesicherten Modus funktionieren nur einige wenige Anwendungen und Windows lädt nur die wichtigsten Treiber und ein Minimum an Betriebssystemkomponenten. Deshalb sind bei einer Verwendung von Windows im abgesicherten Modus die meisten Viren inaktiv und können einfach entfernt werden.

Start von Windows im abgesicherten Modus:

1. Starten Sie Ihren Computer neu.
2. Drücken Sie wiederholt die **F8**-Taste, bevor Windows startet, um so Zugriff auf das Boot-Menü zu erhalten.
3. Wählen Sie **Abgesicherter Modus** im Boot-Menü oder **Abgesicherter Modus mit Netzwerktreibern**, falls Sie Zugang zum Internet haben möchten.
4. Drücken Sie die **Eingabetaste** und warten Sie, während Windows im abgesicherten Modus startet.
5. Dieser Vorgang endet mit einer Bestätigungsbenachrichtigung. Klicken Sie zur Bestätigung auf **OK**.
6. Um Windows normal zu starten, starten Sie einfach Ihr System neu.

DIE SICHERHEITSELEMENTE IM DETAIL

14. VIRENSCHUTZ

Bitdefender schützt Sie vor allen Arten von Malware (Viren, Trojaner, Spyware, Rootkits etc.). Der Virenschutz, den Bitdefender bietet, lässt sich in zwei Kategorien einteilen:

- Zugriff-Scan - Verhindert, dass neue Malware-Bedrohungen auf Ihr System gelangen. Bitdefender wird z.B. ein Worddokument auf Malware scannen, wenn Sie es öffnen oder eine Email-Nachricht, wenn Sie diese empfangen.

  Der Zugriff-Scan stellt den Echtzeitschutz vor Malware sicher und ist damit ein grundlegender Bestandteil jedes Computer-Sicherheitsprogramms.

  Wichtig
  Um zu verhindern, dass Viren Ihren Computer infizieren, sollte der **Zugriff-Scan** immer aktiviert bleiben.

- On-demand Prüfung - erkennt und entfernt Malware die sich bereits auf dem System befindet. Hierbei handelt es sich um einen klassischen, durch den Benutzer gestarteten, Scan - Sie wählen das Laufwerk, Verzeichnis oder Datei, die Bitdefender scannen soll und Bitdefender scannt diese.

Bitdefender scannt automatisch alle Wechselmedien, die mit dem Computer verbunden sind, um einen sicheren Zugriff zu garantieren. Für weitere Informationen lesen Sie bitte *„Automatischer Scan von Wechselmedien“ (S. 95)*.

Erfahrene Benutzer können Scan-Ausschlüsse konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden. Für weitere Informationen lesen Sie bitte *„Konfiguration der Scan-Ausschlüsse“ (S. 97)*.

Wenn Bitdefender einen Virus oder andere Malware feststellt, versucht das Programm automatisch den Malware-Code der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen. Diese Operation bezeichnet man als Desinfektion. Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Für weitere Informationen lesen Sie bitte *„Verwalten von Dateien in Quarantäne“ (S. 100)*.

Wenn Ihr Computer mit Malware infiziert ist, siehe *„Malware von Ihrem System entfernen“ (S. 156)*. Um Ihnen bei der Entfernung von Malware zu helfen, die nicht von innerhalb des Windows-Betriebssystems entfernt werden kann, stellt Bitdefender Ihnen einen Rettungsmodus zur Verfügung. Dabei handelt

es sich um eine vertrauenswürdige Umgebung, die speziell der Entfernung von Malware dient und es Ihnen ermöglicht, Ihren Computer unabhängig von Windows zu starten. Wenn der Computer im Rettungsmodus läuft, ist Windows-Malware inaktiv, wodurch sie sich leicht entfernen lässt.

Um Sie auch vor unbekannten schädlichen Anwendung zu schützen, nutzt Bitdefender mit Active Threat Control eine fortschrittliche heuristische Technologie, die alle Anwendungen auf Ihrem System ununterbrochen überwacht. Active Threat Control blockiert automatisch Anwendungen, die sich wie Malware verhalten, um zu verhindern, dass Sie Ihren Computer beschädigen. Mitunter werden auch legitime Anwendungen blockiert. In diesen Fällen können Sie Active Threat Control durch die Festlegung von Ausschlussregeln so konfigurieren, dass diese Anwendungen nicht noch einmal blockiert werden. Für weitere Informationen lesen Sie bitte das Kapitel *„Active Threat Control“* (S. 101).

14.1. Zugriff-Scans (Echtzeitschutz)

Bitdefender bietet durch die Prüfung aller aufgerufenen Dateien und E-Mail-Nachrichten durchgehenden Echtzeitschutz vor einer Vielzahl von Malware-Bedrohungen.

Die vorgegebenen Einstellungen zum Echtzeitschutz stellen einen guten Schutz gegen Malware bei nur minimaler Beeinträchtigung der Systemleistung sicher. Sie können die Einstellungen zum Echtzeitschutz einfach Ihren Bedürfnissen anpassen, indem Sie eine der vordefinierten Sicherheitsstufe wählen. Wenn Sie ein fortgeschrittener Benutzer sind, können Sie die Scan-Einstellungen auch selbst im Detail konfigurieren, indem Sie eine benutzerdefinierte Schutzstufe definieren.

14.1.1. Aktivieren / Deaktivieren des Echtzeitschutzes

Um den Echtzeitschutz vor Malware zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Schild**.

4. Klicken Sie auf den Schalter, um den Zugriff-Scan zu aktivieren oder deaktivieren.
5. Wenn Sie den Echtzeitschutz deaktivieren, wird ein Warnfenster angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Sie können den Echtzeitschutz für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren. Der Echtzeitschutz wird automatisch nach Ablauf des festgelegten Zeitraums aktiviert.

Warnung
Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen den Echtzeitschutz so kurz wie möglich zu deaktivieren. Während der Echtzeitschutz deaktiviert ist sind Sie nicht vor Schädlingen geschützt.

14.1.2. Echtzeitschutz anpassen

Die Sicherheitsstufe des Echtzeitschutzes definiert die Scan-Einstellungen für den Echtzeitschutz. Sie können die Einstellungen zum Echtzeitschutz einfach Ihren Bedürfnissen anpassen, indem Sie eine der vordefinierten Sicherheitsstufe wählen.

Um die Echtzeitsicherheitsstufe anzupassen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Schild**.
4. Schieben Sie den Regler in die gewünschte Sicherheitsstufenposition. Verwenden Sie die Beschreibung auf der rechten Seite, um die Sicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

14.1.3. Einstellungen des Echtzeitschutzes konfigurieren

Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender nutzen. Sie können die Einstellungen für den Echtzeitschutz im Detail konfigurieren, indem Sie eine benutzerdefinierte Sicherheitsstufe festlegen.

So können Sie die Einstellungen für den Echtzeitschutz anpassen:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Schild**.
4. Klicken Sie auf **Benutzerdefiniert**.
5. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach. Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Scan-Optionen für aufgerufene Dateien.** Sie können Bitdefender so einstellen, dass Dateien oder Anwendungen (Programmdateien) nur bei Zugriff gescannt werden. Das Scannen aller Dateien bietet den besten Schutz, während das ausschließliche Scannen der Anwendungen nur für die Verbesserung der Systemleistung verwendet werden kann.

  Standardmäßig werden sowohl lokale Ordner als auch Netzwerkfreigaben durch Zugriff-Scans gescannt. Wenn Sie Ihre Systemleistung erhöhen möchten, können Sie Netzwerk-Ordner von Zugriff-Scans ausschließen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Diese Kategorie beinhaltet die folgenden Dateierweiterungen:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam;

pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Inhalt von Archiven scannen.** Das Scannen von Archiven ist ein langsamer und ressourcen-intensiver Vorgang, der aus diesem Grund nicht für den Echtzeitschutz empfohlen wird. Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.

  Wenn Sie sich entscheiden, diese Option zu nutzen, können Sie die maximale Größe der Archive angeben, die beim Zugriff-Scan durchsucht werden sollen. Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.

- **Scan-Optionen für E-Mail- und HTTP-Datenverkehr.** Um zu verhindern, dass Malware auf Ihren Computer geladen wird, scannt Bitdefender automatisch die folgenden Malware Einfalltore:
  - eingehende und ausgehende E-Mails
  - HTTP-Datenverkehr

  Das Scannen des Web-Datenverkehrs kann Ihren Webbrowser geringfügig verlangsamen, dadurch können aber über das Internet übertragene Malware, einschließlich Drive-by-Downloads, blockiert werden.

  Sie können zur Steigerung der Systemleistung die Virenschutz-Scans für E-Mail und Internet deaktivieren, dies wird aber nicht empfohlen. Wenn Sie die entsprechenden Scan-Optionen deaktivieren, werden empfangene Emails und aus dem Internet geladene Dateien nicht gescannt. Dies bedeutet aber, dass infizierte Dateien auf Ihrem Computer gespeichert werden können. Dies ist keine bedeutende Bedrohung, da der Echtzeitschutz die Malware blockiert, wenn auf die infizierten Dateien zugegriffen wird (geöffnet, verschoben, kopiert oder ausgeführt).

- **Boot-Sektoren scannen.** Sie können Bitdefender einstellen, damit die Boot-Sektoren gescannt werden. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.

- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Nach Keyloggern suchen.** Wählen Sie diese Option, um Ihr System auf Keylogger zu untersuchen. Keylogger zeichnen auf, was Sie auf Ihrer Tastatur tippen, und schicken dann via Internet Berichte an Hacker. Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.
- **Bei Systemstart scannen.** Wählen Sie die Option "Früher Boot-Scan" aus, um Ihr System bei Systemstart sofort nach dem Laden aller wichtigen Dienste zu scannen. Diese Funktion sorgt für eine bessere Virenerkennung beim Systemstart und beschleunigt diesen zugleich.

Verfügbare Aktionen für gefundene Malware

Sie können einstellen, welche Aktionen der Echtzeit-Schutz ausführen soll.

Führen Sie dazu die folgenden Schritte aus:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Schild**.
4. Klicken Sie auf **Benutzerdefiniert**.
5. Wechseln Sie zum Reiter **Aktionen**, um die Scan-Einstellungen nach Ihrem Bedarf zu konfigurieren.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Der Echtzeit-Schutz in Bitdefender kann die folgenden Aktionen ausführen:

Aktionen ausführen

Bitdefender wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein. Bitdefender wird automatisch versuchen, den Malware-Code

aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diese Operation bezeichnet man als Desinfektion.

Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Für weitere Informationen lesen Sie bitte *„Verwalten von Dateien in Quarantäne“ (S. 100)*.

Wichtig

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Bitdefender versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Dateien in Quarantäne verschieben

Verschiebt die entdeckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem

Grund besteht kein Infektionsrisiko. Für weitere Informationen lesen Sie bitte „*Verwalten von Dateien in Quarantäne*“ (S. 100).

Zugriff verweigern
Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.

14.1.4. Wiederherstellen der Standardeinstellungen

Die vorgegebenen Einstellungen zum Echtzeitschutz stellen einen guten Schutz gegen Malware bei nur minimaler Beeinträchtigung der Systemleistung sicher.

Um die Standardeinstellungen für den Echtzeitschutz wiederherzustellen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Schild**.
4. Klicken Sie auf **Standard**.

14.2. On-Demand Prüfung

Die Aufgabe der Bitdefender-Software ist es sicherzustellen, dass es keine Viren in Ihrem System gibt. Dies wird erreicht, indem neue Viren ferngehalten und Ihre E-Mail-Nachrichten sowie alle heruntergeladenen oder auf Ihr System kopierten Dateien sorgfältig gescannt werden.

Es besteht aber die Gefahr, dass ein Virus bereits in Ihrem System ist, bevor Sie Bitdefender installieren. Deshalb sollten Sie Ihren Computer nach der Installation von Bitdefender auf residente Viren prüfen. Übrigens sollten Sie Ihren Computer auch in Zukunft häufig auf Viren prüfen.

Bedarf-Scans werden über Scan-Aufgaben ausgeführt. Die Scan-Aufgaben beinhalten die Scan-Optionen und die Objekte, die gescannt werden sollen. Sie können den Computer jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen. Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

14.2.1. Eine Datei oder einen Ordner nach Malware scannen

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die/den Sie scannen möchten, wählen Sie **Bitdefender** und dann **Mit Bitdefender scannen**. Der Viren-Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

14.2.2. Durchführen von Quick Scans

Beim Quick Scan wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

Um einen Quick Scan auszuführen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Wählen Sie im Modul **Virenschutz Quick-Scan** aus.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Noch schneller geht es mit einem Klick auf die **Quick-Scan**-Schaltfläche in der Bitdefender-Benutzeroberfläche.

14.2.3. Durchführen von System-Scans

Der System-Scan scannt den gesamten Computer nach allen Malware-Arten wie Viren, Spyware, Adware, Rootkits usw.

Beachten Sie

Da ein **System-Scan** das gesamte System scannt, kann er eine Weile dauern. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie den Computer nicht benötigen.

Bevor Sie einen System-Scan ausführen, sollten Sie Folgendes beachten:

- Vergewissern Sie sich, dass die Malware-Signaturen von Bitdefender auf dem neuesten Stand sind. Ihren Computer unter Verwendung einer veralteten Signaturendatenbank zu prüfen, kann Bitdefender daran hindern neue Maleware, welche seit dem letzten Update gefunden wurde, zu erkennen. Für weitere Informationen lesen Sie bitte *„Bitdefender auf dem neuesten Stand halten“ (S. 46)*.
- Schließen Sie alle geöffneten Programme.

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen. Für weitere Informationen lesen Sie bitte *„Benutzerdefinierte Scans durchführen“ (S. 87)*.

So führen Sie einen System-Scan durch:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Wählen Sie im Modul **Virenschutz System-Scan** aus.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

14.2.4. Benutzerdefinierte Scans durchführen

Um einen Malware-Scan im Detail zu konfigurieren und dann auszuführen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.

3. Wählen Sie im Modul **Virenschutz Scans verwalten** aus.
4. Klicken Sie auf **Neue benutzerdefinierte Aufgabe**. Klicken Sie auf den Reiter **Basic**, um einen Namen für den Scan einzugeben und die Bereiche auszuwählen, die gescannt werden sollen.
5. Um die Scan-Optionen im Detail zu konfigurieren, wählen Sie den Reiter **Erweitert**. Ein neues Fenster wird angezeigt. Folgen Sie diesen Schritten:
   a. Sie können die Scan-Optionen einfach durch Einstellen der Scan-Tiefe festlegen. Schieben Sie den Regler dazu in die gewünschte Position. Die Beschreibung auf der rechten Seite der Skala helfen Ihnen, die Scan-Tiefe zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.

      Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender nutzen. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Benutzerdefiniert**. Weitere Informationen zu den Optionen finden Sie am Ende dieses Kapitels.

   b. Sie können auch folgende allgemeine Optionen konfigurieren:
      - **Aufgabe mit niedriger Priorität ausführen .** Verringert die Priorität des Scan-Vorgangs. Dadurch können andere Programme schneller laufen, der Scan dauert aber länger.
      - **Scan-Assistent in die Task-Leiste minimieren .** Minimiert das Scan-Fenster in die Task-Leiste Es kann durch einen Doppelklick auf das Bitdefender - Logo in der Symbolleiste wieder geöffnet werden.
      - Wählen Sie die Aktion, die durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:

   c. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
6. Klicken Sie im Hauptfenster auf den **Planen**-Schalter im Hauptfenster, um einen Zeitplan für Ihre Scan-Aufgabe festzulegen. Wählen Sie eine der entsprechenden Optionen, um einen Zeitplan festzulegen:
   - Start bei Systemneustart
   - Einmal
   - Periodisch
7. Klicken Sie auf **Scan starten** und folgen Sie den Anweisungen des Assistenten für den Viren-Scan, um den Scan abzuschließen. Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit

in Anspruch nehmen. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

8. Bei Bedarf können Sie einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste klicken.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach. Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Dateien prüfen.** Sie können Bitdefender so einstellen, dass alle Dateitypen oder nur Anwendungen (Programmdateien) gescannt werden. Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Diese Kategorie beinhaltet die folgenden Dateierweiterungen: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Scan-Optionen für Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir

empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

Beachten Sie

Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Boot-Sektoren scannen.** Sie können Bitdefender einstellen, damit die Boot-Sektoren gescannt werden. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen. Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
- **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf Ihrem Computer gespeichert werden.
- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Kommerzielle Keylogger ignorieren.** Wählen Sie diese Option, wenn Sie auf Ihrem Computer eine kommerzielle Keylogger-Software nutzen. Kommerzielle Keylogger sind seriöse Programme zur Überwachung des Computers, deren Hauptfunktion es ist, alle Tastatureingaben aufzuzeichnen.
- **Nach Rootkits suchen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.

14.2.5. Viren-Scan-Assistent

Wann immer Sie einen Bedarf-Scan starten (z. B. indem Sie mit der rechten Maustaste auf einen Ordner klicken, dann Bitdefender und anschließend **Mit Bitdefender scannen** wählen), wird der Bitdefender-Viren-Scan-Assistent eingeblendet. Folgen Sie den Anweisungen des Assistenten, um den Scan-Prozess abzuschließen.

Beachten Sie

Falls der Scan-Assistent nicht erscheint, ist der Scan möglicherweise konfiguriert, im Hintergrund zu laufen. Sehen Sie nach dem Prüffortschritticon im Systemtray. Sie können dieses Objekt anklicken um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Schritt 1 - Führen Sie den Scan durch

Bitdefender startet den Scan der aus gewählten Dateien und Verzeichnisse. Sie erhalten Echtzeitinformationen über den Scan-Status sowie Scan-Statistiken (einschließlich der bisherigen Laufzeit, einer Einschätzung der verbleibenden Laufzeit und der Anzahl der erkannten Bedrohungen).

Bitte warten Sie, bis Bitdefender den Scan beendet hat. Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

Einen Scan anhalten oder unterbrechen. Sie können den Scan-Vorgang jederzeit durch einen Klick auf **Stopp** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Scan-Vorgang vorübergehend anzuhalten, klicken Sie einfach auf **Pause**. Um den Scan-Vorgang fortzusetzen klicken Sie auf **Fortsetzen** .

Passwortgeschützte Archive. Wird ein passwortgeschütztes Archiv gefunden, werden Sie, abhängig von den Scan-Einstellungen, um die Eingabe des Passwortes gebeten. Mit Passwort geschützte Archive können nicht gescannt werden, außer wenn Sie das Passwort angeben. Die folgenden Optionen sind verfügbar:

- **Passwort.** Wenn Sie möchten, dass Bitdefender Archive scannt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach Passwort fragen; das Objekt beim Scan überspringen.** Wählen Sie diese Option um das Scannen diesen Archivs zu überspringen.

- **Alle passwortgeschützten Dateien beim Scan überspringen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. Bitdefender kann diese Dateien und Objekte nicht scannen, erstellt aber einen Eintrag im Scan-Protokoll.

Wählen Sie die gewünschte Option aus und klicken Sie auf **OK**, um den Scan fortzusetzen.

Schritt 2 - Wählen Sie entsprechende Aktionen aus

Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

Beachten Sie

Wenn Sie einen Quick Scan oder einen vollständigen System-Scan durchführen, wird Bitdefender während des Scans automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Die infizierten Objekte werden in Gruppen angezeigt, je nach Malware, mit der sie infiziert sind. Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen. Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktionen ausführen

Bitdefender wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein. Bitdefender wird automatisch versuchen, den Malware-Code aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diese Operation bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem

Grund besteht kein Infektionsrisiko. Für weitere Informationen lesen Sie bitte „*Verwalten von Dateien in Quarantäne*“ (S. 100).

Wichtig

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Bitdefender versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Löschen

Infizierte Dateien werden von der Festplatte entfernt.

Falls infizierte Dateien zusammen mit nicht infizierten Dateien in einem Archiv gespeichert sind, wird Bitdefender versuchen, die infizierten Dateien zu löschen und das Archiv mit den nicht infizierten Dateien zu rekonstruieren. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Keine Aktion ausführen
Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Scan-Vorgang beendet wurde, können Sie das Scan-Protokoll öffnen um Informationen über diese Dateien anzuzeigen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

Schritt 3 - Zusammenfassung

Wenn Bitdefender die Probleme gelöst hat, wird eine Zusammenfassung der Scan-Ergebnisse in einem neuen Fenster angezeigt. Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **Logdatei anzeigen**.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

Wichtig

In den meisten Fällen desinfiziert Bitdefender erfolgreich die aufgespürten infizierten Dateien oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht automatisch gelöst werden können. Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Bereinigungsprozess abgeschlossen werden kann. Weitere Informationen und Anweisungen, wie Sie Malware manuell entfernen können, finden Sie unter *„Malware von Ihrem System entfernen“* (S. 156).

14.2.6. Scan-Protokolle lesen

Bei jedem Scan wird ein Scan-Protokoll erstellt, und Bitdefender zeichnet die gefundenen Probleme im Fenster Virenschutz auf. Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **Protokoll anzeigen** klicken.

Wenn Sie ein Scan-Protokoll lesen oder eine gefundene Infektion einsehen möchten, gehen Sie dazu wie folgt vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
2. Wählen Sie im Fenster **Ereignisanzeige** **Virenschutz** aus dem entsprechenden Menü aus.

Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.

3. In der Ereignisliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
4. Um das Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**. Klicken Sie auf **Erneut scannen**, um einen Scan zu wiederholen.

14.3. Automatischer Scan von Wechselmedien

Bitdefender erkennt automatisch, wenn Sie Wechselmedien mit Ihrem Computer verbinden und scannt diese im Hintergrund. Dies ist empfohlen um die Infizierung Ihres Systems durch Viren und andere Malware zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- verbundene (entfernte) Netzlaufwerke

Sie können den automatischen Scan der Speichermedien eigens für jede Kategorie konfigurieren. Der automatische Scan der abgebildeten Netzlaufwerke ist standardmäßig deaktiviert.

14.3.1. Wie funktioniert es?

Wenn ein Wechseldatenträger erkannt wird, beginnt Bitdefender diesen im Hintergrund nach Malware zu scannen (vorausgesetzt, dass der automatische Scan für diesen Gerätetyp aktiviert ist). Das Bitdefender-Scan-Symbol erscheint in der Task-Leiste. Sie können dieses Objekt anklicken um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Wenn der Auto-Pilot aktiviert ist, läuft der Scan ohne Ihr Zutun. Der Scan wird lediglich protokolliert und Sie können die dazugehörigen Informationen im Ereignis-Fenster abrufen.

Wenn der Autopilot deaktiviert ist:

1. Ein Pop-up-Fenster wird Sie darüber informieren, dass ein neues Gerät erkannt wurde und dass es derzeit gescannt wird.

2. In den meisten Fällen entfernt Bitdefender erkannte Malware automatisch oder isoliert infizierte Dateien in der Quarantäne. Sollte es nach dem Scan noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

   Beachten Sie
   Beachten Sie, dass keine Aktion gegen infizierte oder verdächtige Dateien auf CDs/DVDs vorgenommen werden kann. Ähnlich können keine Aktionen gegen infizierte oder verdächtige Dateien auf Netzlaufwerken vorgenommen werden, wenn Sie nicht die entsprechenden Freigaben haben.

3. Sobald der Scan abgeschlossen ist, wird das Fenster mit den Scan-Ergebnissen angezeigt, um Sie darüber zu informieren, ob Sie die Dateien auf dem Wechselmedium gefahrlos aufrufen können.

Diese Informationen könnten sich als hilfreich erweisen:

- Bitte gehen Sie vorsichtig vor, wenn Sie eine CD oder DVD nutzen, die mit Malware infiziert ist, da diese nicht von dem Datenträger entfernt werden kann (diese Medien sind schreibgeschützt). Stellen Sie sicher, dass der Echtzeitschutz aktiviert ist, um zu verhindern, dass Malware auf Ihr System gelangt. Es empfiehlt sich, wichtige Daten vom Datenträger auf Ihr System zu kopieren und den Datenträger dann zu entsorgen.
- Es kann vorkommen, dass Bitdefender nicht in der Lage ist, Malware aus juristischen oder technischen Gründen aus bestimmten Dateien zu entfernen. Ein Beispiel hierfür sind Dateien, die mithilfe von proprietären Technologien archiviert wurden (der Grund dafür ist, dass das Archiv nicht korrekt wiederhergestellt werden kann).

  Um zu erfahren, wie Sie mit Malware umgehen sollen, lesen Sie bitte das Kapitel *„Malware von Ihrem System entfernen“ (S. 156)*.

14.3.2. Verwalten des Scans für Wechselmedien

Um die automatischen Scans für Wechselmedien zu verwalten, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Ausschlüsse**.

Um den bestmöglichen Schutz zu garantieren, empfiehlt es sich, den automatischen Scan für alle Arten von Wechselmedien zu aktivieren.

Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Wenn infizierte Dateien erkannt werden, wird Bitdefender versuchen, diese zu desinfizieren (d.h. den Malware zu entfernen) oder in die Quarantäne zu verschieben. Sollten beide Maßnahmen fehlschlagen, können Sie im Assistenten für den Virenschutz-Scan andere Aktionen für die infizierten Dateien festlegen. Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

14.4. Konfiguration der Scan-Ausschlüsse

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausschließen. Diese Funktion soll verhindern, dass Sie bei Ihrer Arbeit gestört werden und kann zudem dabei helfen, die Systemleistung zu verbessern. Ausschlüsse sollten nur von Benutzern eingesetzt werden, die erfahren im Umgang mit Computern sind oder wenn dies von einem Bitdefender-Mitarbeiter empfohlen wurde.

Sie können Ausschlüsse so konfigurieren, dass sie für Zugriff-Scans, Bedarf-Scans oder beide Arten von Scans gelten. Die ausgenommenen Objekte werden nicht geprüft, egal ob der Zugriff von Ihnen oder von einem Programm erfolgt.

Beachten Sie

Ausschlüsse werden bei Kontext-Scans NICHT berücksichtigt. Kontextprüfung ist eine Art von On-Demand-Scan: Rechtsklicken Sie auf die zu scannende Datei oder das Verzeichnis und wählen Sie **Mit Bitdefender scannen**.

14.4.1. Dateien oder Ordner vom Scan ausschließen

Um bestimmte Dateien oder Ordner vom Scan auszuschließen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Ausschlüsse** aus.

5. Aktivieren Sie Scan-Ausschlüsse für Dateien durch Anklicken des entsprechenden Schalters.
6. Klicken Sie auf den Link **Ausgeschlossene Dateien und Ordner**. Es erscheint ein Fenster. Hier können Sie die Dateien und Ordner verwalten, die vom Scan ausgeschlossen sind.
7. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Klicken Sie auf **Durchsuchen**, wählen Sie die Datei oder den Ordner, der vom Scan ausgeschlossen werden soll, und klicken Sie auf **OK**. Alternativ können Sie den Datei- oder Ordnerpfad auch manuell (oder per Kopieren und Einfügen) in das Bearbeitungsfeld eingeben.
   c. Standardmäßig werden die ausgewählten Dateien oder Ordner sowohl vom Zugriff-Scan als auch vom Bedarf-Scan ausgeschlossen. Wählen Sie eine der anderen Optionen, um die Anwendung der Ausschlussregel anzupassen.
   d. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

14.4.2. Dateiendungen vom Scan ausschließen

Wenn Sie eine Dateiendung vom Scan ausschließen, wird Bitdefender Dateien mit dieser Endung unabhängig von ihrem Speicherort nicht mehr scannen. Der Ausschluss bezieht sich auch auf Dateien auf Wechselmedien, wie zum Beispiel CDs, DVDs, USB-Sticks oder Netzlaufwerke.

Wichtig
Lassen Sie Vorsichtig walten, wenn Sie Dateiendung vom Scan ausschließen, da solche Ausschlüsse Ihren Computer anfällig für Malware-Bedrohungen machen können.

Um Dateiendungen vom Scan auszuschließen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.

3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Ausschlüsse** aus.
5. Aktivieren Sie Scan-Ausschlüsse für Dateien durch Anklicken des entsprechenden Schalters.
6. Klicken Sie auf den Link **Ausgeschlossene Dateiendungen**. In dem Fenster, das jetzt angezeigt wird, können Sie die Dateiendungen verwalten, die vom Scan ausgenommen sind.
7. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Geben Sie die Dateiendungen ein, die vom Scan ausgeschlossen werden sollen. Trennen Sie einzelne Endungen mit einem Semikolon (;). Hier ein Beispiel:

      txt;avi;jpg

   c. Standardmäßig werden alle Dateien mit den festgelegten Dateiendungen sowohl vom Zugriff-Scan als auch vom Bedarf-Scan ausgeschlossen. Wählen Sie eine der anderen Optionen, um die Anwendung der Ausschlussregel anzupassen.
   d. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

14.4.3. Verwalten von Scan-Ausschlüssen

Werden die konfigurierten Scan-Ausschlüsse nicht mehr benötigt, empfehlen wir, diese zu löschen oder die Scan-Ausschlüsse zu deaktivieren.

Um die Scan-Ausschlüsse zu verwalten, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Ausschlüsse**. Nutzen Sie die Optionen im Bereich **Dateien und Ordner**, um Scan-Ausschlüsse zu verwalten.

4. Um Scan-Ausschlüsse zu entfernen oder zu bearbeiten, klicken Sie auf einen der verfügbaren Links. Gehen Sie wie folgt vor:
   - Um einen Eintrag aus der Tabelle zu entfernen, markieren Sie diesen und klicken dann auf **Entfernen**.
   - Doppelklicken Sie auf einen Tabelleneintrag, um diesen zu bearbeiten(oder markieren Sie den Eintrag und klicken Sie dann auf **Bearbeiten**.) Ein neues Fenster wird angezeigt. Hier können Sie nach Bedarf festlegen, welche Dateiendungen oder -pfade bei welchem Scan-Typ ausgeschlossen werden sollen. Führen Sie die notwendigen Änderungen durch und klicken Sie dann auf **Ändern**.
5. Nutzen Sie den entsprechenden Schalter, um die Scan-Ausschlüsse zu deaktivieren.

14.5. Verwalten von Dateien in Quarantäne

Bitdefender isoliert mit Malware infizierte Dateien, die nicht desinfiziert werden können, sowie verdächtige Dateien in einem sicheren Bereich, der sogenannten Quarantäne. Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

Zudem scannt Bitdefender nach jedem Update der Malware-Signaturen die Dateien der Quarantäne. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

Um Dateien in Quarantäne zu überprüfen und zu verwalten, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Quarantäne**.
4. Dateien in Quarantäne werden von Bitdefender in Übereinstimmung mit den Standardeinstellungen für die Quarantäne automatisch verwaltet. Sie

können die Quarantäneeinstellungen an Ihre Anforderungen anpassen, dies wird aber nicht empfohlen.

Quarantäne nach Signaturupdate erneut scannen
Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch nach jedem Update der Virendefinitionen zu scannen. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

Verdächtige Dateien in Quarantäne zur weiteren Analyse übermitteln
Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch an das Bitdefender-Labor zu schicken. Die Beispieldateien werden dann von den Bitdefender-Malware-Forschern analysiert. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

Inhalte löschen, die älter als {30} Tage sind
Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Wenn Sie diesen Zeitraum verändern möchten, geben Sie einen neuen Wert in das entsprechende Feld ein. Um das automatische Löschen von alten Dateien in Quarantäne zu deaktivieren, geben Sie eine 0 ein.

5. Um eine Quarantäne-Datei zu löschen, markieren Sie diese und klicken dann auf den Button **Löschen**. Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

14.6. Active Threat Control

Active Threat Control von Bitdefender ist eine innovative und vorbeugende Erkennungstechnologie, die hoch entwickelte heuristische Methoden nutzt, um mögliche neue Bedrohungen in Echtzeit zu erkennen.

Active Threat Control überwacht durchgehend alle auf Ihrem Computer laufenden Applikationen auf Aktionen, die auf Malware hindeuten. Jede dieser Aktionen wird eingestuft, für jeden Prozess wird weiterhin eine Allgemeineinstufung erstellt. Wenn diese Gesamteinstufung für einen Prozess einen bestimmten Grenzwert überschreitet, wird der entsprechende Prozess als schädlich eingestuft und automatisch blockiert.

Wenn der Auto-Pilot deaktiviert ist, wird Sie ein Pop-up-Fenster über die blockierte Anwendung informieren. Andernfalls wird die Anwendung ohne

Benachrichtigung blockiert. Im Fenster Ereignisanzeige können Sie überprüfen, welche Anwendungen von Active Threat Control erkannt wurden.

14.6.1. Überprüfen erkannter Anwendungen

So können Sie überprüfen, welche Anwendungen von Active Threat Control erkannt wurden:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
2. Wählen Sie im Fenster **Ereignisanzeige** **Virenschutz** aus dem entsprechenden Menü aus.
3. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
4. Wenn Sie der Anwendung vertrauen, klicken Sie auf **Zulassen und überwachen**, um Active Threat Control so zu konfigurieren, dass sie nicht mehr blockiert wird. Active Threat Control wird ausgeschlossene Anwendungen auch weiterhin überwachen. Wird bei einer ausgeschlossenen Anwendung verdächtiges Verhalten erkannt, wird das Ereignis lediglich protokolliert und als Erkennungsfehler in die Bitdefender-Cloud gemeldet.

14.6.2. Aktivieren / Deaktivieren von Active Threat Control

So können Sie Active Threat Control aktivieren oder deaktivieren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie auf das Modul **Virenschutz**.
4. Wählen Sie im Fenster **Virenschutz** den Reiter **Schild** aus.
5. Klicken Sie auf den Schalter, um Active Threat Control zu aktivieren oder deaktivieren.

14.6.3. Anpassen des Active-Threat-Control-Schutzes

Sollte Ihnen auffallen, das Active Threat Control häufig ungefährliche Anwendung erkennt, sollten Sie eine tolerantere Sicherheitsstufe auswählen.

Schieben Sie den Regler auf die gewünschte Sicherheitsstufenposition, um den Schutz mit Active Threat Control anzupassen.

Verwenden Sie die Beschreibung auf der rechten Seite, um die Sicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

Beachten Sie

Je höher Sie die Sicherheitsstufe einstellen, desto weniger Anzeichen verdächtiger Aktivitäten braucht Active Threat Control, um einen Prozess zu melden. Dadurch steigt die Zahl der gemeldeten Anwendungen, aber auch die Wahrscheinlichkeit von Fehlalarmen (ungefährlichen Anwendungen, die dennoch als schädlich eingestuft wurden).

14.6.4. Verwalten von ausgeschlossenen Prozessen

Sie können Ausschlussregeln für vertrauenswürdige Anwendungen festlegen, damit Active Threat Control diese nicht blockiert, wenn sie sich wie Malware verhalten. Active Threat Control wird ausgeschlossene Anwendungen auch weiterhin überwachen. Wird bei einer ausgeschlossenen Anwendung verdächtiges Verhalten erkannt, wird das Ereignis lediglich protokolliert und als Erkennungsfehler in die Bitdefender-Cloud gemeldet.

So können Sie die Prozesse verwalten, die von Active Threat Control ausgeschlossen wurden:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Ausschlüsse**.
4. Klicken Sie auf den Link **Ausgeschlossene Prozesse**. Ein neues Fenster wird angezeigt. Hier können Sie die Prozesse verwalten, die von Active Threat Control ausgeschlossen wurden.
5. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Klicken Sie auf **Durchsuchen**, wählen Sie die Anwendung, die ausgeschlossen werden soll und klicken Sie dann auf **OK**.
   c. Lassen Sie die **Zulassen**-Option aktiviert, um zu verhindern, dass Active Threat Control die Anwendung blockiert.

d. Klicken Sie auf **Hinzufügen**.

6. Um Ausschlüsse zu entfernen oder zu bearbeiten, gehen Sie folgendermaßen vor:
   - Um ein Objekt aus der Liste zu entfernen markieren Sie es und klicken Sie dann auf die **Entfernen**-Schaltfläche
   - Doppelklicken Sie auf einen Tabelleneintrag, um diesen zu bearbeiten (oder markieren Sie den Eintrag und klicken Sie dann auf **Ändern**.) Führen Sie die notwendigen Änderungen durch und klicken Sie dann auf **Ändern**.
7. Speichern Sie die Änderungen, und schließen Sie das Fenster.

15. INTERNET-SCHUTZ

Der Bitdefender-Internet-Schutz lässt Sie sicher im Web surfen, indem er Sie vor potenziellen Phishing-Seiten warnt.

Bitdefender bietet Echtzeit-Surf-Schutz für:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

So können Sie die Einstellungen für den Internet-Schutz konfigurieren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie auf das Modul **Internet-Schutz**.

Klicken Sie auf die Schalter, um das Folgende zu aktivieren oder deaktivieren:

- Suchberater, eine Komponente, die Ihre Suchmaschinentreffer und Links auf Seiten sozialer Netzwerke analysiert und bewertet. Die Bewertung wird durch ein Symbol neben dem Link oder Treffer angezeigt:

  Sie sollten diese Webseite nicht aufrufen.

  Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.

  Diese Seite ist sicher.

  Der Suchberater anaylsiert die Treffer der folgenden Internet-Suchmaschinen:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Der Suchberater bewertet Links, die auf den folgenden sozialen Netzwerken im Internet veröffentlicht werden:
  - Facebook
  - Twitter

- SSL-Datenverkehr-Scans.

  Gute durchdachte Angriffsversuche könnten den sicheren Datenverkehr für sich zu nutzen, um ihre Opfer zu täuschen. Darum empfiehlt es sich, den SSL-Scan zu aktivieren.

- Schutz vor Betrug.
- Schutz vor Phishing-Attacken.

Sie können eine Liste mit Websites anlegen, die nicht von den Bitdefender-Engines für den Malware-, Phishing- und Betrugsschutz gescannt werden sollen. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen. Fügen Sie beispielsweise Websites hinzu, auf denen Sie häufig einkaufen.

Um Websites mithilfe des Internet-Schutzes in Bitdefender zu konfigurieren und verwalten, klicken Sie auf den Link zur **Whitelist**. Ein neues Fenster wird angezeigt.

Um eine Website zur Whitelist hinzuzufügen, geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Hinzufügen**.

Um eine Website aus der Liste zu entfernen, wählen Sie sie aus der Liste aus und klicken Sie auf den entsprechenden **Entfernen**-Link.

Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

15.1. Bitdefender-Benachrichtigungen im Browser

Wenn Sie versuchen eine Website aufzurufen, die als unsicher eingestuft wurde, wird die entsprechende Website blockiert und eine Warnseite wird in Ihrem Browser angezeigt.

Die Seite enthält Informationen wie zum Beispiel die URL der Website und die erkannte Bedrohung.

Sie müssen entscheiden, wie Sie fortfahren möchten. Die folgenden Optionen sind verfügbar:

- Die Seite über einen Klick auf **Ich gehe lieber auf Nummer sicher** verlassen.
- Die Blockierung von Seiten, die Phishing-Elemente enthalten, mit einem Klick auf **Phishing-Filter deaktivieren** aufheben.
- Die Blockierung von Seiten, die Malware enthalten, mit einem Klick auf **Malware-Filter deaktivieren** aufheben.

- Fügen Sie die Seite der Phishing-Schutz-Whitelist hinzu, indem Sie auf **Zur Whitelist hinzufügen** klicken. Diese Seite wird nicht mehr von den Phishing-Schutz-Engines von Bitdefender gescannt.
- Rufen Sie die Website trotz der Warnung auf, indem Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken.

16. IDENTITÄTSSCHUTZ

16.1. Endgültiges Löschen von Dateien

Wenn Sie eine Datei löschen, kann auf diese nicht mehr auf normalem Wege zugegriffen werden. Die Datei ist jedoch physisch solange weiterhin auf der Festplatte vorhanden, bis sie durch eine neue Datei überschrieben wird.

Der Bitdefender-Dateischredder hilft Ihnen, Daten endgültig zu löschen, indem er sie physisch von der Festplatte entfernt.

Wenn Sie das Windows-Kontextmenü nutzen möchten, um Dateien oder Ordner auf Ihrem Computer schnell und einfach zu schreddern, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, den Sie unwiderruflich löschen möchten.
2. Wählen Sie dann im Kontextmenü **Bitdefender** > **Dateischredder**.
3. Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **Ja**, um den Assistenten für den Dateischredder zu starten.
4. Bitte warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.
5. Die Ergebnisse werden angezeigt. Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Alternativ können Sie Dateien auch von innerhalb der Bitdefender-Benutzeroberfläche schreddern.

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Privatsphäre**.
3. Wählen Sie im Modul **Datenschutz** den Punkt **Dateischredder** aus.
4. Befolgen Sie die Anweisungen des Dateischredderassistenten:
   a. **Ordner hinzufügen**

      Fügen Sie die Dateien oder Verzeichnisse, die Sie endgültig entfernen möchten, hinzu.

b. Klicken Sie auf **Weiter** und bestätigen Sie, dass Sie den Vorgang fortsetzen möchten.

   Bitte warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.

c. **Bericht**

   Die Ergebnisse werden angezeigt. Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

17. SCHWACHSTELLEN

Ein wichtiger Schritt für den Schutz Ihres Computers gegen Hacker und schädliche Anwendungen besteht darin, das Betriebssystem und die Programme, die Sie oft verwenden, stets auf dem neusten Stand eu halten. Sie sollten zudem in Betracht ziehen, die Windows-Einstellungen zu deaktivieren, die das System anfälliger für Malware machen. Und um einen ungewünschten Zugriff auf Ihren Computer zu vermeiden sind sichere Passwörter (Passwörter die nicht einfach umgangen werden können) für jedes Windows-Benutzerkonto notwendig.

Bitdefender überprüft Ihr System automatisch auf Schwachstellen und informiert Sie über diese. Systemschwachstellen beinhalten das Folgende:

- veraltete Anwendungen auf Ihrem Computer.
- fehlende Windows Updates.
- Schwache Windows Benutzerkonten Passwörter.

Bitdefender bietet Ihnen zwei einfache Möglichkeiten, die Schwachstellen Ihres Systems zu beheben:

- Sie können Ihr System nach Schwachstellen durchsuchen und diese Schritt für Schritt mit dem **Schwachstellen-Scan** beheben.
- Mithilfe der automatischen Schwachstellenüberwachung können Sie im Ereignis-Fenster erkannte Schwachstellen überprüfen und beheben.

Sie sollten Ihr System alle ein bis zwei Wochen nach Schwachstellen durchsuchen und diese beheben.

17.1. Scannen des Computers nach Schwachstellen

So beheben Sie Systemschwachstellen mit dem Schwachstellen-Scan:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Schwachstelle** auf **Schwachstellen-Scan**.
4. Bitte warten Sie, bis Bitdefender die Schwachstellenprüfung beendet hat. Klicken Sie unten im Fenster auf **Überspringen**, um den Scan-Vorgang zu beenden.

Noch schneller geht es mit einem Klick auf die **Quick-Scan**-Schaltfläche in der Bitdefender-Benutzeroberfläche.

- **Kritische Windows-Updates**

  Klicken Sie auf **Details anzeigen**, um die Liste aller wichtigen Windows-Updates anzuzeigen, die zur Zeit nicht auf Ihrem Computer installiert sind.

  Um die Installation der gewählten Updates zu starten, klicken Sie auf **Updates installieren**. Bitte beachten Sie, dass die Installation der Updates einige Zeit in Anspruch nehmen kann und dass manche Updates einen Neustart erfordern, um die Installation abzuschließen. Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

- **Anwendungsupdates**

  Wenn eine Anwendung nicht auf dem neusten Stand ist, klicken Sie auf **Neue Version herunterladen**, um die aktuellste Version herunterzuladen.

  Klicken Sie auf **Details anzeigen**, um Informationen zu der Anwendung anzuzeigen, die aktualisiert werden muss.

- **Unsichere Passwörter für Windows-Benutzerkonten**

  Sie können die Liste der auf Ihrem Computer konfigurierten Windows-Benutzerkonten sehen und die Sicherheit, die das jeweilige Passwort bietet.

  Klicken Sie auf **Passwortwechsel beim Login**, um ein neues Passwort für Ihr System festzulegen.

  Klicken Sie auf **Details anzeigen**, um unsichere Passwörter zu ändern. Sie können den jeweiligen Benutzer auffordern, das Passwort bei der nächsten Anmeldung zu ändern oder das Passwort sofort selbst ändern. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).

Oben rechts im Fenster können Sie die Ergebnisse entsprechend Ihrer Anforderungen filtern.

17.2. Automatische Schwachstellenüberwachung

Bitdefender scannt Ihr System im Hintergrund regelmäßig nach Schwachstellen und erfasst alle erkannten Probleme im Ereignis-Fenster.

Um die erkannten Probleme zu untersuchen und zu beheben, gehen Sie folgendermaßen vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Ereignisanzeige** aus dem Menü aus.
2. Wählen Sie im Fenster **Ereignisanzeige** unter Ereignisse auswählen den Punkt **Schwachstelle** aus.
3. Sie erhalten detaillierte Informationen zu den erkannten Systemschwachstellen. Abhängig vom Problem, um eine spezifische Schwachstelle zu beheben, gehen Sie folgendermaßen vor:
   - Falls Windows-Updates verfügbar sind, klicken Sie auf **Jetzt aktualisieren**.
   - Klicken Sie auf **Aktivieren**, falls automatische Windows-Updates deaktiviert wurden.
   - Falls eine Anwendung nicht mehr auf dem neuesten Stand ist, klicken Sie auf **Update jetzt durchführen**, um einen Link zur Website des Anbieters zu finden, von der aus Sie die neueste Version der Anwendung installieren können.
   - Wenn ein Windows-Benutzerkonto mit einem schwachen Passwort gesichert ist, klicken Sie auf **Passwort ändern**, um den Benutzer dazu zu zwingen, das Passwort bei der nächsten Anmeldung zu ändern oder es selbst zu ändern. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).
   - Sollte die Autorun-Funktion in Windows aktiviert sein, klicken Sie auf **Beheben**, um sie zu deaktivieren.

Um die Einstellungen für die Schwachstellenüberwachung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie auf das Modul **Schwachstelle**.
4. Klicken Sie auf den Schalter, um den Schwachstellen-Scan zu aktivieren oder deaktivieren.

Wichtig
Um automatisch über System- oder Anwendungsschwachstellen benachrichtigt zu werden, lassen Sie die Option **Schwachstellen-Scan** aktiviert.

5. Nutzen Sie die entsprechenden Schalter, um die Systemschwachstellen auszuwählen, die Sie regelmäßig überprüfen möchten.

   Kritische Windows-Updates
   Überprüfen Sie, ob die neuesten kritischen Microsoft-Sicherheits-Updates auf Ihrem Windows-Betriebssystem installiert sind.

   Anwendungsupdates
   Prüfen Sie, ob die auf Ihren System installierten Anwendungen aktuell sind. Veraltete Anwendungen können von schädlicher Software ausgenutzt werden und Ihren PC so anfällig für Angriffe von außen machen.

   Unsichere Passwörter
   Überprüfen Sie, ob die Passwörter der Windows-Benutzerkonten, leicht zu erraten sind oder nicht. Passwörter, die schwer zu erraten sind (starke Passwörter), mache es sehr schwierig für Hacker, in Ihr System einzudringen. Ein starkes Passwort sollte aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen (z.B. #, $ oder @) bestehen.

   Medien-Autostart
   Überprüfen Sie den Status der Windows-Autorun-Funktion. Mit dieser Funktion lassen sich Anwendungen automatisch direkt von CD, DVD, USB-Stick oder anderen externen Speichermedien starten.

   Manche Malware-Arten verbreiten sich über den Autostart von Wechselmedien auf Ihrem PC. Aus diesem Grund sollten Sie diese Windows-Funktion deaktivieren.

Beachten Sie
Wenn Sie die Überwachung einer bestimmten Schwachstelle deaktivieren, werden damit zusammenhängende Ereignisse nicht mehr im Ereignisfenster erfasst.

18. RANSOMWARE-SCHUTZ

Bei Ransomware handelt es sich um Schadsoftware, die anfällige Systeme infiziert und den Zugriff darauf sperrt. Von den Benutzern wird dann für die Freigabe ihrer Daten ein Lösegeld erpresst. Diese Schadsoftware geht intelligent vor und zeigt Benutzern gefälschte Warnmeldungen an, um sie in Angst zu versetzen und sie dazu zu bringen, das geforderte Geld zu zahlen.

Übertragen werden kann die Infektion durch das Herunterladen von Anhängen an Spam-Nachrichten oder durch das Aufrufen infizierter Websites und die Installation von schädlichen Anwendungen, ohne dass der Benutzer überhaupt merkt, was auf seinem System vorgeht.

Ransomware kann den Benutzer auf die folgenden Arten aus seinem System aussperren:

- Verschlüsselung sensibler und persönlicher Dateien, die erst nach Zahlung durch das Opfer wieder entschlüsselt werden können.
- Sperren des Bildschirms und Anzeige einer Benachrichtigung, die ebenfalls die Zahlung eines Geldbetrags fordert. In diesen Fällen erfolgt keine Verschlüsselung der Dateien, der Benutzer wird jedoch dennoch gezwungen, die Zahlung vorzunehmen.
- Verhindert die Ausführung von Anwendungen.

Der Ransomware-Schutz von Bitdefender setzt auf neueste Technologien, um die Integrität des Systems zu gewährleisten. Dabei werden kritische Systembereiche vor Schäden geschützt, die sich auf das gesamte System auswirken. Darüber hinaus sollten Sie auch Ihre persönlichen Daten wie Dokumente, Fotos, Filme oder in der Cloud gespeicherte Dateien schützen.

18.1. Aktivieren und Deaktivieren des Ransomware-Schutzes

So können die das Modul für den Ransomware-Schutz deaktivieren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie auf **Ransomware-Schutz**.

4. Klicken Sie auf den Schalter, um den **Ransomware-Schutz** zu aktivieren oder deaktivieren.

Versucht eine Anwendung nun, auf eine geschützte Datei zuzugreifen, wird ein Bitdefender-Pop-up-Fenster angezeigt. Sie können den Zugriff erlauben oder verweigern.

Beachten Sie
Der Ransomware-Schutz ist standardmäßig aktiviert.

18.2. Schützen Sie Ihre persönlichen Dateien vor Ransomware-Angriffen.

So können Sie Ihre persönlichen Daten sicher geschützt verwahren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie auf das Modul für den **Ransomware-Schutz** und danach auf die **Geschützte Ordner**-Schaltfläche.
4. Klicken Sie auf **Hinzufügen** und rufen Sie den Ordner auf, den Sie schützen möchten.
5. Klicken Sie auf **OK**, um den ausgewählten Ordner zur geschützten Umgebung hinzuzufügen.

Die Ordner Eigene Dokumente, Eigene Bilder, Öffentliche Dokumente und Öffentliche Bilder werden standardmäßig vor Malware-Angriffen geschützt. Sofern die entsprechenden Anwendungen auf dem System installiert sind, können auch bei File-Hosting-Diensten wie Box, Dropbox, Google Drive und OneDrive gespeicherte Daten zur geschützten Umgebung hinzugefügt werden.

Beachten Sie
Benutzerdefinierte Ordner können nur für den aktuellen Benutzer geschützt werden. System- und Anwendungsdateien können den Ausschlüssen nicht hinzugefügt werden.

18.3. Konfiguration vertrauenswürdiger Anwendungen

Sie können den Ransomware-Schutz für bestimmte Anwendungen deaktivieren, Sie sollten sich aber sicher sein, dass es sich dabei um vertrauenswürdige Anwendungen handelt.

So können Sie vertrauenswürdige Anwendungen zu den Ausschlüssen hinzufügen:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Ransomware-Schutz** auf **Vertrauenswürdige Anwendungen**.
4. Klicken Sie auf **Hinzufügen** und wählen Sie die Anwendungen aus, die Sie schützen möchten.
5. Klicken Sie auf **OK**, um die ausgewählte Anwendung zur geschützten Umgebung hinzuzufügen.

18.4. Konfiguration blockierter Anwendungen

Einige der auf Ihrem Computer installierten Anwendungen werden versuchen, auf Ihre persönlichen Dateien zuzugreifen.

So können Sie den Zugriff durch diese Anwendungen einschränken:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Ransomware-Schutz** auf **Blockierte Anwendungen**.
4. Klicken Sie auf **Hinzufügen** und wählen Sie die Anwendungen aus, die Sie einschränken möchten.
5. Klicken Sie auf **OK**, um die ausgewählte Anwendung zur Liste der eingeschränkten Anwendungen hinzuzufügen.

18.5. Schutz beim Systemstart

Viele Malware-Anwendungen sind bekanntermaßen darauf ausgelegt, beim Systemstart ausgeführt zu werden, und können einen Computer so ernsthaft beschädigen. Der Bitdefender-Systemstartschutz scannt alle kritischen Systembereiche noch bevor alle Dateien geladen werden, ohne dabei die Systemleistung zu beeinträchtigen. Gleichzeitig werden Sie so vor bestimmten Angriffsarten geschützt, die auf die Ausführung von Heap-Code, Code Injection oder Hooks in bestimmten dynamischen Bibliotheken setzen.

So können Sie den Systemstartschutz deaktivieren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie auf **Ransomware-Schutz**.
4. Klicken Sie auf den Schalter, um den **Schutz beim Systemstart** zu aktivieren oder deaktivieren.

19. SICHERE ONLINE-TRANSAKTIONEN MIT SAFEPAY

Immer mehr Menschen nutzen ihren Computer regelmäßig für ihre Einkäufe und Bankgeschäfte. Rechnungen bezahlen, Überweisungen tätigen und einkaufen war noch nie schneller und einfacher.

Bei diesen Transaktionen werden personenbezogene Daten, Konto- und Kreditkartennummern, Passwörter und andere vertrauliche Informationen über das Internet übermittelt. Und das sind genau die Daten, die Online-Kriminelle so gerne in die Finger kriegen würden. Hacker lassen nichts unversucht, an diese Daten zu gelangen. Sie können also bei der Absicherung Ihrer Online-Transaktionen gar nicht vorsichtig genug sein.

Bitdefender Safepay™ ist zuallererst ein gesicherter Browser, ein abgeschottetes System, das speziell entwickelt wurde, damit Online-Transaktionen wie Einkäufe und Bankgeschäfte sicher und privat bleiben.

Um optimalen Privatsphärenschutz zu gewährleisten, wurde der Bitdefender-Passwortmanager in Bitdefender Safepay™ integriert, um Ihre Anmeldedaten jederzeit beim Aufrufen von privaten Seiten zu schützen. Für weitere Informationen lesen Sie bitte *„Passwortmanager-Schutz für Ihre Anmeldedaten“* (S. 123).

Bitdefender Safepay™ hat die folgenden Vorteile:

- Es blockiert den Zugriff auf Ihren Desktop sowie sämtliche Versuche, Bildschirmfotos zu machen.
- So werden Ihre Passwörter im Internet mit dem Passwortmanager geschützt.
- Es hat eine eingebaute virtuelle Tastatur, die es Hackern unmöglich macht, Ihre Tastenanschläge aufzuzeichnen.
- Es ist völlig unabhängig von Ihren anderen Browsern.
- Es enthält den Hotspot-Schutz für Situationen, in denen Ihr Computer mit einem ungesicherten Funknetzwerk verbunden ist.
- Es hat eine Lesezeichenfunktion, mit der Sie mühelos auf Ihre Lieblings-Banking/Shopping-Seiten zugreifen können.
- Es ist nicht nur auf Online-Banking und -Shopping beschränkt. Jede Webseite kann in Bitdefender Safepay™ geöffnet werden.

19.1. Bitdefender Safepay™ verwenden

Standardmäßig erkennt Bitdefender, wenn Sie auf Ihrem Computer über einen Browser eine Online-Banking-Seite oder einen Online-Shop aufrufen und fordert Sie auf, diese Seite in Bitdefender Safepay™ zu öffnen.

Es gibt verschiedene Möglichkeiten, das Bitdefender Safepay™-Hauptfenster zu öffnen:

- Über die Bitdefender-Benutzeroberfläche:
  1. Klicken Sie in der Bitdefender-Benutzeroberfläche auf die **Safepay**-Schaltfläche.
- In Windows:
  - In **Windows 7**:
    1. Klicken Sie auf **Start** und **Alle Programme**.
    2. Klicken Sie auf **Bitdefender**.
    3. Klicken Sie auf **Bitdefender Safepay™**.
  - In **Windows 8 und Windows 8.1**:

    Finden Sie Bitdefender Safepay™ auf der Windows-Startseite (z.B. durch die Eingabe von "Bitdefender Safepay™" auf der Startseite) und rechtsklicken Sie auf das Symbol.
  - In **Windows 10**:

    Geben Sie "Bitdefender Safepay™" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.

> **Beachten Sie**
> Falls das Adobe Flash Player Plugin nicht installiert oder nicht mehr aktuell ist, wird eine Bitdefender-Meldung angezeigt. Klicken Sie auf die entsprechende Schaltfläche, um fortzufahren.
> Nach Abschluss des Installationsvorgangs müssen Sie den Bitdefender Safepay™-Browser erneut öffnen, um mit Ihrer Arbeit fortzufahren.

Wer schon einmal einen Internet-Browser benutzt hat, wird mit Bitdefender Safepay™ keinerlei Probleme haben - es sieht aus wie ein Browser und verhält sich auch so:

- Sie können URLs in die Adressleiste eingeben, um auf die entsprechende Seite zu gelangen.

- Sie können im Fenster von Bitdefender Safepay™ mehrere Reiter öffnen, indem Sie auf klicken.
- Sie können über die Schaltflächen rückwärts und vorwärts durch bereits besuchte Seiten blättern und Seiten neu laden.
- die Bitdefender Safepay™-Einstellungen aufrufen, indem Sie auf klicken und **Einstellungen** auswählen.
- schützen Sie Ihre Passwörter mit dem Passwortmanager durch einen Klick auf .
- Sie können Ihre Lesezeichen mit einem Klick auf neben der Adressleiste verwalten.
- Sie können eine virtuelle Tastatur über die Schaltfläche öffnen.
- die Größe des Browser-Fensters durch gleichzeitiges Drücken von **Strg** und den **+/-**-Tasten im numerischen Tastenblock anpassen.
- Informationen über Ihr Bitdefender-Produkt aufrufen, indem Sie auf auf **Info über** auswählen.
- wichtige Informationen ausdrucken mit einem Klick auf .

19.2. Einstellungen verändern

Klicken Sie auf und danach auf **Einstellungen**, um Bitdefender Safepay™ zu konfigurieren:

Allgemeine Einstellungen

Hier können Sie einstellen, was passiert, wenn Sie die Seite eines Online-Shops oder eine Internet-Banking-Seite in einem normalen Browser aufrufen:

- Websites automatisch in Safepay öffnen.
- Verwendung von Safepay empfehlen.
- Verwendung von Safepay nicht empfehlen.

Domain-Liste

Hier können Sie einstellen, wie Bitdefender Safepay™ sich verhalten soll, wenn Sie Webseiten bestimmter Domains in Ihrem Standardbrowser aufrufen. Fügen Sie dazu einzelne Domains der Liste hinzu, und wählen Sie für jede eines der folgenden Verhalten:

- Automatisch in Bitdefender Safepay™ öffnen.
- Bitdefender soll Sie jedes Mal fragen, wie Sie vorgehen möchten.

- Bitdefender Safepay™ beim Aufruf von Seiten dieser Domain in einem Standardbrowser nie benutzen.

Blockieren von Pop-ups

Pop-ups können Sie mit einem Klick auf den entsprechenden Schalter blockieren.

Sie können auch eine Liste mit Websites anlegen, die Pop-ups anzeigen dürfen. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen.

Um eine Website zu der Liste hinzuzufügen, geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Domain hinzufügen**.

Um eine Website aus der Liste zu entfernen, wählen Sie sie aus der Liste aus und klicken Sie auf den entsprechenden **Entfernen**-Link.

Aktivieren des Hotspot-Schutzes

Durch Aktivierung dieser Funktion können Sie bei Verbindungen mit ungeschützten WLAN-Netzwerken eine weitere Schutzebene hinzufügen.

Unter *„Hotspot-Sicherheit in ungesicherten Netzwerken“ (S. 122)* erhalten Sie weitere Informationen.

19.3. Lesezeichen verwalten

Wenn Sie die automatische Erkennung einiger oder aller Websites deaktiviert haben oder Bitdefender einfach bestimmte Websites nicht korrekt erkennt, können Sie in Bitdefender Safepay™ Lesezeichen anlegen und so in Zukunft häufig besuchte Seiten schneller aufrufen.

So fügen Sie eine URL zu den Lesezeichen von Bitdefender Safepay™ hinzu:

1. Klicken Sie auf das -Symbol neben der Adressleiste, um die Lesezeichenliste zu öffnen.

   Beachten Sie
   Die Lesezeichenliste wird standardmäßig geöffnet, wenn Sie Bitdefender Safepay™ starten.

2. Klicken Sie auf das **+** um ein neues Lesezeichen hinzuzufügen.
3. Geben Sie die URL und den Titel für das Lesezeichen ein, und klicken Sie anschließend auf **Erstellen**. Aktivieren Sie die Option **Automatisch in Safepay öffnen**, wenn die in den Lesezeichen gespeicherte Seite bei jedem

Besuch mit Bitdefender Safepay™ geöffnet werden soll. Die URL wird auch in der Domain-Liste auf der Seite Einstellungen hinzugefügt.

19.4. Hotspot-Sicherheit in ungesicherten Netzwerken

Wenn Sie Bitdefender Safepay™ in einem ungesicherten Funknetzwerk nutzen (z. B. an einem öffentlichen Hotspot) kann die Funktion Hotspot-Schutz zusätzliche Sicherheit bieten. Dieser Dienst verschlüsselt die Internetkommunikation über ungesicherte Verbindungen, sodass Ihre Privatsphäre geschützt bleibt, ganz gleich, in welchem Netzwerk Sie sich befinden.

Der Hotspot-Schutz funktioniert nur dann, wenn der Computer mit einem ungeschützten Netzwerk verbunden ist.

Die sichere Verbindung wird aufgebaut; im Bitdefender Safepay™-Fenster wird dann eine Nachricht angezeigt, sobald die Verbindung steht. Das Symbol wird in der Adressleiste vor der URL angezeigt, wenn es sich um eine sichere Verbindung handelt.

Um das Surfen im Internet visuell ansprechender zu gestalten, können Sie **Adobe Flash**- und **Java**-Plug-ins aktivieren, indem Sie auf **Erweiterte Einstellungen anzeigen** klicken.

Sie müssen die Aktion vielleicht bestätigen.

20. PASSWORTMANAGER-SCHUTZ FÜR IHRE ANMELDEDATEN

Wir nutzen unsere Computer, um im Internet einzukaufen, unsere Rechnungen zu bezahlen, soziale Netzwerke zu besuchen oder Sofortnachrichten zu verschicken.

Aber wie jeder weiß, kann es manchmal schwer sein, sich alle Passwörter zu merken!

Und wenn wir bei Surfen im Internet nicht vorsichtig sind, können wir unsere privaten Daten wie E-Mail-Adresse, Chat-Name oder Kreditkarteninformationen ungewollt preisgeben.

Passwörter und persönliche Daten aufzuschreiben oder auf dem Computer zu speichern, kann gefährlich sein, weil sie dort nicht vor Unbefugten sicher sind, die es auf diese Informationen abgesehen haben. Und es ist eine echte Herausforderung, sich jedes einzelne Passwort zu merken, das Sie für Ihre Online-Konten und Lieblingsseiten festgelegt haben.

Gibt es also eine Möglichkeit, unsere Passwörter zu aufzubewahren, dass wir jederzeit darauf zugreifen können? Und können wir sicher sein, dass unsere Passwörter auch geheim bleiben?

Der Passwortmanager hilft Ihnen, nie wieder ein Passwort zu vergessen. Zudem schützt er Ihre Privatsphäre und garantiert ein sicheres Internet-Vergnügen.

Durch die Verwendung eines Master-Passworts für den Zugriff auf Ihre Anmeldedaten schützt der Passwortmanager Ihre Passwörter zuverlässig in einer Geldbörse.

Um Ihre Online-Aktivitäten optimal abzusichern, ist der Passwortmanager mit Bitdefender Safepay™ integriert und bietet eine einheitliche Lösung für den Schutz vor den vielen Bedrohungen, denen Ihre Daten ausgesetzt sind.

Mit dem Passwortmanager können die folgenden privaten Daten geschützt werden:

- Persönliche Daten wie zum Beispiel E-Mail-Adressen oder Telefonnummern
- Anmeldeinformationen für verschiedene Websites
- Kontonummern oder Kreditkarteninformationen
- Informationen zu E-Mail-Konten

- Anwendungspasswörter
- WLAN-Passwörter

20.1. Konfiguration des Passwortmanagers

Nach Abschluss der Installation werden Sie beim Öffnen des Browsers informiert, dass die Geldbörse jetzt einsatzbereit ist.

In der Bitdefender-Geldbörse können Sie Ihre persönlichen Daten speichern.

Klicken Sie auf **Durchsuchen**, um den Installationsassistenten für die Geldbörse zu starten. Folgen Sie den Anweisungen des Assistenten, um den Installationsvorgang abzuschließen.

In diesem Schritt haben Sie zwei Optionen:

- Eine neue Geldbörsen-Datenbank erstellen, um Ihre Passwörter zu schützen.

  Während des Installationsvorgangs werden Sie aufgefordert, Ihre Geldbörse mit einem Master-Passwort zu schützen. Wählen Sie ein sicheres Passwort mit mindestens 7 Zeichen.

  Ein sicheres Passwort beinhaltet mindestens eine Zahl oder ein Sonderzeichen sowie einen Großbuchstaben. Sobald Sie ein Passwort festgelegt haben, muss jeder, der die auf die Geldbörse zugreifen will, zunächst das Passwort eingeben.

  Nach Festlegung eines Master-Passworts können Sie die in der Geldbörse gespeicherten Daten in der Cloud synchronisieren, um sie auf allen Ihren Geräten nutzen zu können.

  Nach Abschluss des Installationsvorgangs sind die folgenden Einstellungen für die Geldbörse standardmäßig aktiviert:

  - **Anmeldedaten automatisch in der digitalen Geldbörse speichern**.
  - **Nach meinem Master-Passwort fragen, wenn ich mich an meinem Computer anmelde**.
  - **Die Geldbörse automatisch sperren, wenn ich meinen PC verlasse**.
- Eine bestehende Datenbank importieren, wenn Sie die Geldbörse bereits zuvor verwendet haben.

Die Geldbörse-Datenbank exportieren

Um Ihre Geldbörse-Datenbank zu exportieren, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Privatsphäre**.
3. Rufen Sie das **Passwortmanager**-Modul auf und wechseln Sie zum Reiter **Geldbörse**.
4. Wählen Sie die gewünschte Geldbörse-Datenbank im Bereich **Meine Geldbörse** aus und klicken Sie auf **Exportieren**.
5. Folgen Sie den Anweisungen, um die Geldbörse-Datenbank an einen lokalen Speicherort zu exportieren.

Beachten Sie

Die Geldbörse muss geöffnet sein, damit die Schaltfläche für den **Export**angezeigt wird.

Neue Geldbörsen-Datenbank erstellen

Um eine neue Geldbörsen-Datenbank zu erstellen, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Privatsphäre**.
3. Rufen Sie das **Passwortmanager**-Modul auf und wechseln Sie zum Reiter **Geldbörse**.
4. Klicken Sie im angezeigten Fenster auf +.
5. Klicken Sie unter **Von vorn beginnen** auf **Neu anlegen**.
6. Geben Sie die Daten in die entsprechenden Felder ein.
   - Geldbörsenbezeichnung - Geben Sie Ihrer Geldbörse-Datenbank einen eindeutigen Namen
   - Master-Passwort - Geben Sie ein Passwort für Ihre Geldbörse ein.

- Passwort wiederholen - Wiederholen Sie das angegebene Passwort.
- Hinweis - Geben Sie einen Passworthinweis ein.

7. Klicken Sie auf **Fortfahren**.
8. An diesem Punkt können Sie angeben, ob Sie Ihre Informationen in der Cloud speichern möchten. Wenn Sie Ja auswählen, werden Ihre Bankdaten auch weiterhin lokal auf Ihrem Gerät gespeichert werden. Wählen Sie die gewünschte Option aus und klicken Sie auf **Fortfahren**.
9. Wählen Sie den Web-Browser aus, aus dem Sie die Anmeldedaten importieren möchten.
10. Klicken Sie auf **Fertigstellen**.

Synchronisieren Ihrer Geldbörsen in der Cloud

So können Sie die Geldbörse-Synchronisation in der Cloud aktivieren oder deaktivieren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Privatsphäre**.
3. Rufen Sie das **Passwortmanager**-Modul auf und wechseln Sie zum Reiter **Geldbörse**.
4. Wählen Sie die gewünschte Geldbörse-Datenbank im Bereich **Meine Geldbörse** aus und klicken Sie auf **Einstellungen**.
5. Ein neues Fenster wird angezeigt. Wählen Sie die gewünschte Option aus und klicken Sie auf **Speichern**.

> **Beachten Sie**
> Die Geldbörse muss geöffnet sein, damit die Schaltfläche für die **Einstellungen**angezeigt wird.

Geldbörse-Anmeldedaten verwalten

Um Ihre Passwörter zu verwalten, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.

2. Wechseln Sie zum Reiter **Privatsphäre**.
3. Rufen Sie das **Passwortmanager**-Modul auf und wechseln Sie zum Reiter **Geldbörse**.
4. Wählen Sie die gewünschte Geldbörse-Datenbank im Bereich **Meine Geldbörse** aus und klicken Sie auf **Öffnen**.

Ein neues Fenster wird angezeigt. Wählen Sie im Fenster oben die gewünschte Kategorie aus:

- Identität
- Webseiten
- Online-Banking
- EMails
- Anwendungen
- WLAN

Hinzufügen/Bearbeiten von Anmeldedaten

- Um ein neues Passwort hinzuzufügen, wählen Sie oben die entsprechende Kategorie aus, klicken Sie auf **+ Objekt hinzufügen**, geben Sie die Informationen in den entsprechenden Feldern ein und klicken Sie auf Speichern.
- Um ein Objekt aus der Liste zu bearbeiten, klicken Sie auf die **Bearbeiten**-Schaltfläche.
- Klicken Sie zum Verlassen auf **Abbrechen**.
- Um einen Eintrag zu entfernen, wählen Sie ihn aus, klicken Sie auf **Bearbeiten** und wählen Sie **Löschen**.

20.2. Aktivieren oder Deaktivieren des Passwortmanager-Schutzes

So können Sie den Passwortmanager-Schutz aktivieren oder deaktivieren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Privatsphäre**.

3. Rufen Sie das **Passwortmanager**-Modul auf.
4. Klicken Sie auf den Schalter **Modulstatus**, um den Passwortmanager zu aktivieren oder deaktivieren.

20.3. Verwaltung der Passwortmanager-Einstellungen

Um das Master-Passwort im Detail zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Privatsphäre**.
3. Rufen Sie das **Passwortmanager**-Modul auf und wechseln Sie zum Reiter **Sicherheitseinst.**.

Die folgenden Optionen sind verfügbar:

- **Nach meinem Master-Passwort fragen, wenn ich mich an meinem PC anmelde** - Sie werden aufgefordert, Ihr Master-Passwort beim Zugriff auf den Computer anzugeben.
- **Nach meinem Master-Passwort fragen, wenn ich meine Browser und Anwendungen öffne** - Sie werden aufgefordert, Ihr Master-Passwort beim Zugriff auf den Browser oder eine Anwendung anzugeben.
- **Die Geldbörse automatisch sperren, wenn ich meinen PC verlasse** - Sie werden aufgefordert, Ihr Master-Passwort anzugeben, wenn Sie nach 15 Minuten an Ihren Computer zurückkehren.

Wichtig

Merken Sie sich Ihr Master-Passwort gut oder schreiben Sie es auf und verwahren es an einem sicheren Ort. Wenn Sie Ihr Passwort vergessen haben, müssen Sie das Programm neu installieren oder den Kundendienst von Bitdefender kontaktieren.

Machen Sie es sich noch einfacher

So können Sie die Browser oder Anwendungen auswählen, die mit dem Passwortmanager integriert werden sollen:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.

2. Wechseln Sie zum Reiter **Privatsphäre**.
3. Rufen Sie das **Passwortmanager**-Modul auf und wechseln Sie zum Reiter **Plugins**.

   Wählen Sie eine Anwendung für die Nutzung des Passwortmanagers aus und machen Sie es sich noch einfacher:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay
   - Skype
   - Yahoo! Messenger

Konfigurieren des automatischen Einfügens

Die Funktion für das automatische Einfügen erleichtert Ihnen den Zugriff auf Ihre Lieblingsseiten und das Anmelden bei Ihren Online-Konten. Ihre Anmeldedaten und persönlichen Daten werden bei der ersten Eingabe in Ihrem Web-Browser automatisch in der Geldbörse sicher gespeichert.

Um die Einstellungen für das **automatische Einfügen** zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Privatsphäre**.
3. Rufen Sie das **Passwortmanager**-Modul auf und wechseln Sie zum Reiter **Einstellungen autom. Einfügen.**.
4. Entscheiden Sie sich für eine der folgenden Optionen:
   - **Anmeldedaten automatisch einfügen**:
     - **Anmeldedaten immer automatisch einfügen** - Die Anmeldedaten werden automatisch im Browser eingefügt.
     - **Jedes Mal nachfragen, ob meine Anmeldedaten automatisch eingefügt werden sollen** - Sie entscheiden, ob Ihre Anmeldedaten automatisch im Browser eingefügt werden.

- **Legen Sie fest, wie der Passwortmanager Ihre Anmeldedaten absichern soll**:
  - **Anmeldedaten automatisch in der digitalen Geldbörse speichern** - Anmeldedaten und andere persönlich identifizierbare Daten wie Personendaten oder Kreditkarteninformationen werden in der Geldbörse automatisch gespeichert und aktualisiert.
  - **Immer fragen** - Sie werden jedes Mal gefragt, ob Ihre Anmeldedaten zur Geldbörse hinzugefügt werden sollen.
  - **Nicht speichern, ich möchte die Informationen manuell aktualisieren** - Die Anmeldedaten können nur von Hand zur Geldbörse hinzugefügt werden.
- **Formulare automatisch ausfüllen**:
  - **Auf Formularseiten meine Ausfülloptionen anzeigen** - Ein Pop-up-Fenster mit Ihren Ausfülloptionen wird angezeigt, sobald Bitdefender erkennt, dass Sie eine Online-Zahlung vornehmen oder sich anmelden wollen.

Passwortmanager-Daten über Ihren Browser verwalten

Sie können den Passwortmanager direkt über Ihren Browser verwalten, um jederzeit auf alle wichtigen Daten zugreifen zu können. Das Bitdefender-Geldbörse-Add-on wird von den folgenden Browsern unterstützt: Google Chrome, Internet Explorer und Mozilla Firefox. Darüber hinaus ist es auch in Safepay integriert

Um auf die Bitdefender-Geldbörse-Erweiterung zugreifen zu können, öffnen Sie Ihren Web-Browser, stimmen Sie der Installation des Add-ons zu und klicken Sie in der Symbolleiste auf das -Symbol.

Die Bitdefender-Geldbörse-Erweiterung bietet die folgenden Optionen:

- Geldbörse öffnen - Öffnet die Geldbörse.
- Geldbörse sperren - Sperrt die Geldbörse.
- Webseiten - Öffnet ein Untermenü mit allen in der Geldbörse gespeicherten Website-Anmeldedaten. Klicken Sie auf **Webseite hinzufügen**, um neue Websites zu der Liste hinzuzufügen.

- Formulare ausfüllen - Öffnet ein Untermenü mit den Informationen, die Sie für eine bestimmte Kategorie hinzugefügt haben. Hier können Sie neue Daten zu Ihrer Geldbörse hinzufügen.
- Passwortgenerator - Mit dem Passwortgenerator können Sie Zufallspasswörter für bestehende und neue Benutzerkonten erstellen. Klicken Sie auf **Erweiterte Einstellungen anzeigen**, um die Passwortkomplexität selbst zu konfigurieren.
- Einstellungen - Öffnet das Fenster für die Passwortmanager-Einstellungen.
- Problem melden - Hier können Sie alle Probleme melden, die im Zusammenhang mit dem Bitdefender-Passwortmanager auftreten.

21. USB IMMUNIZER

Die Autostart-Funktion, die in jedem Windows-Betriebssystem angelegt ist, ist sehr praktisch, denn über sie kann der Computer direkt Dateien auf angeschlossenen Medien ausführen. So werden zum Beispiel eine Installation sofort gestartet, wenn die Installations-CD der Software eingelegt wird.

Leider kann Schad-Software diese Funktion missbrauchen, um sich automatisch von beschreibbaren Medien wie USB-Sticks und Speicherkarten aus auf Ihrem System einzunisten. In der letzten Zeit ist die Zahl der Angriffe über die Autostart-Funktion gewachsen.

Mit der USB-Immunisierung können Sie verhindern, dass mit NTFS, FAT32 oder FAT formatierte Flash-Speicher je wieder automatisch Malware ausführen. Wenn ein USB-Gerät einmal immunisiert wurde, kann es nicht mehr durch Malware dazu gebracht werden, eine bestimmte Anwendung auszuführen, sobald es mit einem Windows-Computer verbunden wird.

So können Sie ein USB-Gerät immunisieren:

1. Verbinden Sie das Flash-Laufwerk mit Ihrem Computer.
2. Suchen Sie das Gerät auf Ihrem Arbeitsplatz und klicken Sie mit der rechten Maustaste darauf.
3. Wählen Sie im Kontextmenü **Bitdefender** und anschließend **Dieses Laufwerk immunisieren**.

> **Beachten Sie**
> Wenn das Laufwerk bereits immunisiert wurde, wird anstatt der Immunisierungsoption folgende Meldung angezeigt: **Das USB-Gerät ist gegen Autostart-Malware geschützt.**

Sie können auch verhindern, dass Ihr Computer Malware von nicht immunisierten USB-Geräten startet, indem Sie die Autostart-Funktion deaktivieren. Für weitere Informationen lesen Sie bitte *„Automatische Schwachstellenüberwachung“* (S. 111).

SYSTEMOPTIMIERUNG

22. PROFILE

Das Arbeiten, Filme schauen oder Spielen am Computer kann das System verlangsamen, ganz besonders dann, wenn diese Aktivitäten mit Windows-Update-Vorgängen oder Wartungsaufgaben einhergehen. Mit Bitdefender können Sie jetzt ein bevorzugtes Profil auswählen und anwenden und damit Ihr System so anpassen, dass die jeweils benötigten Anwendungen optimal laufen.

Bitdefender bietet die folgenden Profile:

- Arbeitsprofil
- Filmprofil
- Spielprofil

Falls Sie sich entscheiden, die **Profile** nicht zu nutzen, wird ein voreingestelltes Profil mit dem Namen **Standard** aktiviert, dass Ihr System nicht optimiert.

In Übereinstimmung mit Ihrer Aktivität werden die folgenden Produkteinstellungen vorgenommen, wenn ein Profil aktiviert wird:

- Alle Bitdefender-Alarme und Pop-ups sind deaktiviert.
- Automatische Updates werden verschoben.
- Geplante Scans werden verschoben.
- Der Suchberater wird deaktiviert.
- Benachrichtigungen zu Sonderangeboten und Produktbenachrichtigungen sind deaktiviert.

In Übereinstimmung mit Ihrer Aktivität werden die folgenden Systemeinstellungen vorgenommen, wenn ein Profil aktiviert wird:

- Automatische Windows-Updates werden verschoben.
- Windows-Benachrichtigungen und Pop-ups sind deaktiviert.
- Nicht benötigte Hintergrundprogramme werden angehalten.
- Die visuellen Effekte werden für maximale Leistung optimiert.
- Wartungsaufgaben werden verschoben.
- Die Energiespareinstellungen werden angepasst.

22.1. Arbeitsprofil

Das gleichzeitige Ausführen von verschiedenen Aufgaben bei der Arbeit am PC, so zum Beispiel das Versenden von E-Mails, das Abhalten von Videokonferenzen mit Kollegen oder das Arbeiten mit Grafikprogrammen, können die Leistung Ihres Systems beeinträchtigen. Das Arbeitsprofil wurde entwickelt, um Sie effizienter arbeiten zu lassen. Dafür werden einige Hintergrunddienste und Wartungsaufgaben deaktiviert.

Konfigurieren des Arbeitsprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Arbeitsprofil:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Klicken Sie im Fenster **Profileinstellungen** auf die **Konfigurieren**-Schaltfläche im Bereich Arbeitsprofil.
5. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für Arbeitsanwendungen steigern
   - Produkteinstellungen für das Arbeitsprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben
   - Automatische Windows-Updates später durchführen
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Manuelles Hinzufügen von Anwendungen zur Arbeitsprofilliste

Wenn das Arbeitsprofil im Bitdefender beim Aufrufen einer Arbeitsanwendung nicht automatisch aktiviert wird, können Sie die Anwendung manuell zu der **Anwendungsliste** hinzufügen.

So fügen Sie Anwendungen manuell zur Anwendungsliste im Arbeitsprofil hinzu:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Klicken Sie im Modul **Profile** auf die **Konfigurieren**-Schaltfläche im Bereich Arbeitsprofil.
4. Klicken Sie im Fenster **Arbeitsprofil** auf den Link zur **Anwendungsliste**.
5. Klicken Sie auf **Hinzufügen**, um eine neue Anwendung zur **Anwendungsliste** hinzuzufügen.

   Ein neues Fenster wird angezeigt. Scrollen Sie bitte bis zu der ausführbaren Datei der Anwendung, wählen Sie diese aus und klicken Sie auf **OK**, um diese zu der Liste hinzuzufügen.

22.2. Filmprofil

Das Abspielen von Videos mit hoher Qualität, so zum Beispiel HD-Filme, nimmt viele Systemressourcen in Anspruch. Mit dem Filmprofil werden die System- und Produkteinstellungen so angepasst, dass Sie Ihre Filme ungestört genießen können.

Konfigurieren des Filmprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Filmprofil:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Klicken Sie im Fenster **Profileinstellungen** auf die **Konfigurieren**-Schaltfläche im Bereich Filmprofil.
5. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für das Abspielen von Videos steigern
   - Produkteinstellungen für das Filmprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben

- Automatische Windows-Updates später durchführen
- Energiesparplaneinstellungen für den Filmbetrieb anpassen

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Manuelles Hinzufügen von Video-Playern zur Filmprofilliste

Wenn das Filmprofil im Bitdefender beim Aufrufen eines Video-Players nicht automatisch aktiviert wird, können Sie den Player manuell zu der **Player-Liste** hinzufügen.

So fügen Sie Video-Player manuell zur Player-Liste im Filmprofil hinzu:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Klicken Sie im Modul **Profile** auf die **Konfigurieren**-Schaltfläche im Bereich Filmprofil.
4. Klicken Sie im Fenster **Filmprofil** auf den Link zur **Player-Liste**.
5. Klicken Sie auf **Hinzufügen**, um einen neuen Player zur **Player-Liste** hinzuzufügen.

   Ein neues Fenster wird angezeigt. Scrollen Sie bitte bis zu der ausführbaren Datei der Anwendung, wählen Sie diese aus und klicken Sie auf **OK**, um diese zu der Liste hinzuzufügen.

22.3. Spielprofil

Um Ihre Spiele ohne Unterbrechungen genießen zu können, müssen Systemunterbrechungen und Leistungseinbußen unbedingt minimiert werden. Durch die Kombination von verhaltensbasierten Heuristiken und einer Liste bekannter Spiele kann Bitdefender automatisch erkennen, ob ein Spiel ausgeführt wird, und Ihre Systemressourcen so optimieren, dass Sie in Ruhe spielen können.

Konfigurieren des Spielprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Spielprofil:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Klicken Sie auf das Modul **Profile**.
4. Klicken Sie im Fenster **Profileinstellungen** auf die **Konfigurieren**-Schaltfläche im Bereich Spielprofil.
5. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für Spiele steigern
   - Produkteinstellungen für das Spielprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben
   - Automatische Windows-Updates später durchführen
   - Energiesparplaneinstellungen für den Spielbetrieb anpassen
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Spiele manuell zu der Spielliste hinzufügen

Wenn das Spielprofil im Bitdefender beim Aufrufen eines Spiels oder einer Anwendung nicht automatisch aktiviert wird, können Sie die Anwendung manuell zu der **Spieleliste** hinzufügen.

So fügen Sie Spiele manuell zur Spieleliste im Spielprofil hinzu:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Klicken Sie im Modul **Profile** auf die **Konfigurieren**-Schaltfläche im Bereich Spielprofil.
4. Klicken Sie im Fenster **Spielprofil** auf den Link zur **Spieleliste**.
5. Klicken Sie auf **Hinzufügen**, um ein neues Spiel zur **Spieleliste** hinzuzufügen.

Ein neues Fenster wird angezeigt. Öffnen Sie den Ordner, in dem sich die ausführbare Datei des Spiels befindet, markieren Sie sie und klicken Sie auf **OK**, um das Spiel zur Liste hinzuzufügen.

22.4. Echtzeitoptimierung

Die Bitdefender-Echtzeitoptimierung ist ein Plug-in, das Ihre Systemleistung unbemerkt im Hintergrund verbessert und so sicherstellt, dass Sie im Profile-Modus nicht gestört werden. Je nach CPU-Auslastung überwacht das Plug-in alle Prozesse und konzentriert sich dabei auf Prozesse, die Ihr System überdurchschnittlich belasten, um sie an Ihre Anforderungen anzupassen.

So können Sie die Echtzeitoptimierung aktivieren oder deaktivieren:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Extras**.
3. Klicken Sie im Modul **Profile** auf den Reiter **Profileinstellungen**.
4. Aktivieren oder deaktivieren Sie die Echtzeitoptimierung, indem Sie auf den entsprechenden Schalter klicken.

PROBLEMLÖSUNG

23. VERBREITETE PROBLEME BEHEBEN

In diesem Kapitel werden einige Probleme, die Ihnen bei der Verwendung von Bitdefender begegnen können, erläutert. Zudem finden Sie hier Lösungsvorschläge für diese Probleme. Die meisten dieser Probleme können über eine passende Konfiguration der Produkteinstellungen gelöst werden.

- *„Mein System scheint langsamer zu sein“* (S. 141)
- *„Der Scan startet nicht“* (S. 143)
- *„Ich kann eine Anwendung nicht mehr ausführen“* (S. 145)
- *„Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert?“* (S. 147)
- *„Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann“* (S. 147)
- *„Mein Computer ist nicht mit dem Internet verbunden. Wie kann ich Bitdefender aktualisieren?“* (S. 148)
- *„Bitdefender-Dienste antworten nicht“* (S. 149)
- *„Das automatische Einfügen funktioniert bei meiner Geldbörse nicht“* (S. 150)
- *„Entfernen von Bitdefender ist fehlgeschlagen“* (S. 151)
- *„Mein System fährt nach der Installation von Bitdefender nicht mehr hoch“* (S. 152)

Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Bitdefender wie in Kapitel *„Hilfe anfordern“* (S. 166) beschrieben, kontaktieren.

23.1. Mein System scheint langsamer zu sein

Nach der Installation einer Sicherheitssoftware ist eine geringfügige Verlangsamung des Systems bis zu einem gewissen Grad normal.

Wenn Sie eine erhebliche Systemverlangsamung feststellen, kann dies folgende Ursachen haben:

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software.**

  Obwohl Bitdefender bereits auf Ihrem System installierte Sicherheitsprogramme während der Installation sucht und entfernt,

empfehlen wir dennoch, jedes andere Virenschutzprogramm von Ihrem Rechner zu entfernen, bevor Sie die Installation von Bitdefender starten. Für weitere Informationen lesen Sie bitte *„Wie entferne ich andere Sicherheitslösungen?“ (S. 74).

- **Die Mindestsystemanforderungen für die Ausführung von Bitdefender sind nicht erfüllt.**

  Wenn Ihr PC die Mindestsystemanforderungen nicht erfüllt, verlangsamt dies Ihr System, insbesondere dann, wenn mehrere Anwendungen gleichzeitig laufen. Für weitere Informationen lesen Sie bitte *„Mindestsystemanforderungen“ (S. 3)*.

- **Sie haben Anwendungen auf Ihrem Computer, die Sie nicht nutzen**.

  Auf jedem Computer befinden sich Programme oder Anwendungen, die Sie nicht benutzen. Im Hintergrund laufen viele unerwünschte Programme, die Speicherplatz und Arbeitsspeicher beanspruchen. Wenn Sie ein Programm nicht nutzen, deinstallieren Sie es. Das gilt auch für vorinstallierte Software oder Testversionen, die Sie nicht wieder entfernt haben.

  Wichtig
  Wenn Sie glauben, dass ein Programm oder eine Anwendung ein wichtiger Bestandteil Ihres Betriebssystems ist, entfernen Sie es nicht und wenden Sie sich an den Bitdefender-Kundendienst.

- **Ihr System ist vielleicht infiziert**.

  Die Geschwindigkeit und das allgemeine Verhalten Ihres Systems kann auch durch Malware beeinträchtigt werden. Spyware, Viren, Trojaner und Adware wirken sich negativ auf Ihre Systemleistung aus. Stellen Sie sicher, dass Ihr System regelmäßig gescannt wird, mindestens einmal pro Woche. Es empfiehlt sich, einen Bitdefender-System-Scan durchzuführen, da so nach allen Malware-Typen gesucht wird, die die Sicherheit Ihres Systems bedrohen.

  Um den System-Scan zu starten, gehen Sie folgendermaßen vor:

  1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
  2. Wechseln Sie zum Reiter **Schutz**.

3. Wählen Sie im Modul **Virenschutz System-Scan** aus.
4. Befolgen Sie die Anweisungen des Assistenten.

23.2. Der Scan startet nicht

Dieses Problem kann folgende Ursachen haben:

- **Eine vorherige Installation von Bitdefender wurde nicht vollständig entfernt oder es handelt sich um eine fehlerhafte Bitdefender-Installation**.

  Befolgen Sie dafür die folgenden Schritte:

  1. Entfernen Sie Bitdefender vollständig von Ihrem System:
     - In **Windows 7**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
       b. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
       c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
       d. Klicken Sie auf **Weiter**.
       e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
     - In **Windows 8 und Windows 8.1**:
       a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
       b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
       c. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
       d. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
       e. Klicken Sie auf **Weiter**.
       f. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 10**:
  a. Klicken Sie auf **Start** und danach auf Einstellungen.
  b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
  c. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
  d. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
  e. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
  f. Klicken Sie auf **Weiter**.
  g. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

2. Installieren Sie Ihr Bitdefender-Produkt erneut.

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software**.

  Befolgen Sie dafür die folgenden Schritte:

  1. Entfernen Sie die andere Sicherheitslösung. Für weitere Informationen lesen Sie bitte *„Wie entferne ich andere Sicherheitslösungen?“* (S. 74).
  2. Entfernen Sie Bitdefender vollständig von Ihrem System:
     - In **Windows 7**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
       b. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
       c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
       d. Klicken Sie auf **Weiter**.
       e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
     - In **Windows 8 und Windows 8.1**:

a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

c. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.

d. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

e. Klicken Sie auf **Weiter**.

f. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 10**:

a. Klicken Sie auf **Start** und danach auf Einstellungen.

b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

c. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.

d. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

e. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

f. Klicken Sie auf **Weiter**.

g. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

3. Installieren Sie Ihr Bitdefender-Produkt erneut.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt „*Hilfe anfordern*“ (S. 166) beschrieben.

23.3. Ich kann eine Anwendung nicht mehr ausführen

Dieses Problem tritt auf, wenn Sie versuchen, ein Programm zu verwenden, das vor der Installation von Bitdefender einwandfrei funktioniert hatte.

Nach der Installation von Bitdefender könnten folgende Situationen eintreten:

- Sie könnten einen Benachrichtigung von Bitdefender erhalten, dass das Programm versucht, Veränderungen am System durchzuführen.
- Es ist möglich, dass Sie von dem Programm, das Sie starten möchten, eine Fehlermeldung erhalten.

Diese Situation tritt ein, wenn Active Threat Control eine Anwendung fälschlicherweise als Malware einstuft.

Active Threat Control ist ein Bitdefender-Modul, das ständig die laufenden Programme Ihres Systems überwacht und einen Bericht über jene sendet, die sich potenziell gefährlich verhalten. Da diese Funktion auf dem heuristischen System basiert, kann es Fälle geben, in denen einwandfreie Anwendungen im Bericht der Active Threat Control aufgelistet werden.

In solchen Fällen können Sie die entsprechende Anwendung von der Überwachung durch Active Threat Control ausschließen.

Wenn Sie das Programm der Ausschlussliste hinzufügen möchten, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie im Modul **Virenschutz** auf den Reiter **Ausschlüsse**.
4. Klicken Sie auf den Link **Ausgeschlossene Prozesse**. Ein neues Fenster wird angezeigt. Hier können Sie die Prozesse verwalten, die von Active Threat Control ausgeschlossen wurden.
5. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Klicken Sie auf **Durchsuchen**, wählen Sie die Anwendung, die ausgeschlossen werden soll und klicken Sie dann auf **OK**.
   c. Lassen Sie die **Zulassen**-Option aktiviert, um zu verhindern, dass Active Threat Control die Anwendung blockiert.
   d. Klicken Sie auf **Hinzufügen**.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt „*Hilfe anfordern*“ (S. 166) beschrieben.

23.4. Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert?

Bitdefender ermöglicht Ihnen sicheres Surfen im Netz, indem es den Internet-Datenverkehr filtert und schädliche Inhalte blockiert. Es kann jedoch auch vorkommen, dass Bitdefender eine sichere Website oder Online-Anwendung als unsicher einstuft, wodurch diese dann durch den Bitdefender-Scan des HTTP-Datenverkehrs irrtümlich blockiert werden.

Sollte die gleiche Seite oder Anwendung wiederholt blockiert werden, können Sie diese zu einer sogenannten Whitelist hinzufügen, damit sie von den Bitdefender-Engines nicht mehr gescannt werden. So können Sie ungestört im Internet surfen.

So fügen Sie eine Website zur **Whitelist** hinzu:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Klicken Sie auf das Modul **Internet-Schutz**.
4. Klicken Sie im Reiter **Einstellungen** auf den Link **Whitelist**.
5. Geben Sie die Adresse der blockierten Website oder Online-Anwendung in das entsprechende Feld ein und klicken Sie **Hinzufügen**.
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Sie sollten dieser Liste nur Websites und Anwendungen hinzufügen, denen Sie auch wirklich vertrauen. Diese werden dann von den folgenden Engines vom Scan ausgeschlossen: Malware, Phishing und Betrug.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 166)* beschrieben.

23.5. Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann

Falls Sie über eine langsame Internet-Verbindung (wie z. B. ein Modem) verfügen, können während des Updates Fehler auftreten.

Um Ihr System hinsichtlich Bitdefender-Malware-Signaturen auf dem neuesten Stand zu halten, gehen Sie folgendermaßen vor:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **Allgemeine Einstellungen** aus dem Menü aus.
2. Wählen Sie im Fenster **Allgemeine Einstellungen** den Reiter **Update** aus.
3. Wählen Sie neben **Update-Verarbeitungsregeln** den Eintrag **Vor dem Download nachfragen** aus dem Menü aus.
4. Kehren Sie zum Bitdefender-Hauptfenster zurück und klicken Sie hier auf die Schaltfläche **Update**.
5. Wählen Sie nur **Signatur-Updates** und klicken Sie dann auf **OK**.
6. Bitdefender wird nur die Malware-Signatur-Updates herunterladen und installieren.

23.6. Mein Computer ist nicht mit dem Internet verbunden. Wie kann ich Bitdefender aktualisieren?

Wenn Ihr Computer über keine Internet-Verbindung verfügt, müssen Sie die Updates manuell auf einen Computer mit Internet-Zugang herunterladen und dann über einen Wechseldatenträger wie beispielsweise einen USB-Speicherstick auf Ihren Rechner transferieren.

Folgen Sie diesen Schritten:

1. Öffnen Sie auf einem Computer mit Internet-Zugang einen Web-Browser und gehen Sie auf:

   http://www.bitdefender.de/site/view/Desktop-Products-Updates.html

2. Klicken Sie in der Spalte **Manuelles Update** auf den entsprechenden Link für Ihr Produkt und Ihre Systemarchitektur. Wenn Sie nicht wissen, ob auf Ihrem Computer eine 32-Bit- oder 64-Bit-Version von Windows ausgeführt wird, lesen Sie bitte *„Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?“ (S. 73)*.
3. Speichern Sie die Datei namens weekly.exe im System.
4. Übertragen Sie die heruntergeladene Datei zunächst auf einen Wechseldatenträger wie beispielsweise einen USB-Speicherstick und dann auf Ihren Computer.

5. Doppelklicken Sie auf die Datei und folgen Sie den Anweisungen des Assistenten.

23.7. Bitdefender-Dienste antworten nicht

Dieser Artikel hilft Ihnen bei der Lösung des Problems **Bitdefender-Dienste antworten nicht**. Sie könnten folgende Fehlermeldung erhalten:

- Das Bitdefender-Symbol im der Task-Leiste ist grau hinterlegt und Sie erhalten eine Meldung, dass die Bitdefender-Dienste nicht reagieren.
- Das Bitdefender-Fenster zeigt an, dass die Bitdefender-Dienste nicht antworten.

Der Fehler kann durch einen der folgenden Umstände verursacht werden:

- Temporäre Kommunikationsstörungen zwischen den Bitdefender-Diensten.
- Einige der Bitdefender-Dienste wurden angehalten.
- Andere Sicherheitslösungen laufen gleichzeitig mit Bitdefender auf Ihrem Rechner.

Um diesen Fehler zu beheben, versuchen Sie folgenden Lösungen:

1. Warten Sie einen Moment und beobachten Sie, ob sich etwas ändert. Der Fehler könnte vorübergehend sein.
2. Starten Sie den Rechner neu und warten Sie einige Momente, bis Bitdefender geladen ist. Öffnen Sie Bitdefender und überprüffen Sie ob das Problem immernoch besteht. Durch einen Neustart des Computers wird das Problem normalerweise gelöst.
3. Überprüfen Sie, ob Sie irgendeine andere Sicherheitslösung installiert haben, weil diese den Normalbetrieb von Bitdefender stören könnte. Wenn dies der Fall ist, empfehlen wir Ihnen alle anderen Sicherheitslösungen zu entfernen und Bitdefender wieder neu zu installieren.

   Für weitere Informationen lesen Sie bitte *„Wie entferne ich andere Sicherheitslösungen?“* (S. 74).

Sollte der Fehler weiterhin auftreten, wenden Sie sich bitte an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“* (S. 166) beschrieben.

23.8. Das automatische Einfügen funktioniert bei meiner Geldbörse nicht

Sie haben Ihre Online-Anmeldedaten bereits in Ihrer Bitdefender-Geldbörse gespeichert und das automatische Einfügen funktioniert nicht. Dieses Problem tritt in der Regel auf, wenn die Erweiterung für den Bitdefender-Passwortmanager in Ihrem Browser nicht installiert wurde.

Um das Problem zu beheben, gehen Sie folgendermaßen vor:

- Im **Internet Explorer:**
  1. Öffnen Sie den Internet Explorer.
  2. Klicken Sie auf Extras.
  3. Klicken Sie auf Add-Ons verwalten.
  4. Klicken Sie auf Symbolleisten und Erweiterungen.
  5. Bewegen Sie den Mauszeiger auf **Bitdefender-Passwortmanager** und klicken Sie Aktivieren.
- In **Mozilla Firefox:**
  1. Öffnen Sie Mozilla Firefox.
  2. Klicken Sie auf Extras.
  3. Klicken Sie auf Add-ons.
  4. Klicken Sie auf Erweiterungen.
  5. Bewegen Sie den Mauszeiger auf **Bitdefender-Passwortmanager** und klicken Sie Aktivieren.
- In **Google Chrome:**
  1. Öffnen Sie Google Chrome.
  2. Klicken Sie auf das Menü-Symbol.
  3. Klicken Sie auf Einstellungen.
  4. Klicken Sie auf Erweiterungen.
  5. Bewegen Sie den Mauszeiger auf **Bitdefender-Passwortmanager** und klicken Sie Aktivieren.

Beachten Sie
Das Add-on wird nach einem Neustart des Browsers aktiviert.

Überprüfen Sie jetzt, ob das automatische Einfügen für Ihre Online-Benutzerkonten funktioniert.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 166)* beschrieben.

23.9. Entfernen von Bitdefender ist fehlgeschlagen

Wenn Sie Ihr Bitdefender-Produkt deinstallieren möchten und Sie bemerken, dass der Prozess hängen bleibt oder das System einfriert, klicken Sie auf **Abbrechen**. Sollte dies nicht zum Erfolg führen, starten Sie den Computer neu.

Falls die Deinstallation fehlschlägt, bleiben unter Umständen einige Bitdefender-Registry-Schlüssel und Dateien in Ihrem System. Solche Überbleibsel können eine erneute Installation von Bitdefender verhindern. Ebenso kann die Systemleistung und Stabilität leiden.

Um Bitdefender vollständig von Ihrem System zu entfernen, gehen Sie folgendermaßen vor:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
  3. Wählen Sie zunächst **Entfernen** und danach **Ich möchte es dauerhaft entfernen** aus.
  4. Klicken Sie auf **Weiter**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

3. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
4. Wählen Sie zunächst **Entfernen** und danach **Ich möchte es dauerhaft entfernen** aus.
5. Klicken Sie auf **Weiter**.
6. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
  3. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
  5. Wählen Sie zunächst **Entfernen** und danach **Ich möchte es dauerhaft entfernen** aus.
  6. Klicken Sie auf **Weiter**.
  7. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

23.10. Mein System fährt nach der Installation von Bitdefender nicht mehr hoch

Wenn Sie Bitdefender gerade installiert haben und Ihr System nicht mehr im Normalmodus starten können, kann es verschiedene Ursachen für dieses Problem geben.

Höchstwahrscheinlich wird es durch eine vorherige Bitdefender-Installation hervorgerufen, die nicht vollständig entfernt wurde. Eine weitere Möglichkeit ist eine andere Sicherheitslösung, die noch auf dem System installiert ist.

Im Folgenden finden Sie Herangehensweisen für die verschiedenen Situationen:

- **Sie hatten Bitdefender schon einmal im Einsatz und danach nicht vollständig von Ihrem System entfernt.**

Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 76).
2. Entfernen Sie Bitdefender von Ihrem System:
   - In **Windows 7**:
     a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
     b. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
     c. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
     d. Klicken Sie auf **Weiter**.
     e. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.
     f. Starten Sie Ihren Computer im Normalmodus neu.
   - In **Windows 8 und Windows 8.1**:
     a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
     b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
     c. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.
     d. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.
     e. Klicken Sie auf **Weiter**.
     f. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.
     g. Starten Sie Ihren Computer im Normalmodus neu.
   - In **Windows 10**:
     a. Klicken Sie auf **Start** und danach auf Einstellungen.

b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

c. Suchen Sie **Bitdefender Antivirus Plus 2016** und wählen Sie **Deinstallieren**.

d. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

e. Klicken Sie im angezeigten Fenster auf **Entfernen** und wählen Sie danach **Ich möchte es erneut installieren** aus.

f. Klicken Sie auf **Weiter**.

g. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.

h. Starten Sie Ihren Computer im Normalmodus neu.

3. Installieren Sie Ihr Bitdefender-Produkt erneut.

- **Sie hatten zuvor eine andere Sicherheitslösung im Einsatz und haben diese nicht vollständig entfernt.**

  Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

  1. Starten Sie Ihren Computer im abgesicherten Modus neu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 76).

  2. Entfernen Sie die andere Sicherheitslösung von Ihrem System:

     - In **Windows 7**:

       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.

       b. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.

       c. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

     - In **Windows 8 und Windows 8.1**:

       a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

       b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.

d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

- In **Windows 10**:

a. Klicken Sie auf **Start** und danach auf Einstellungen.

b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.

d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie dann Ihr System neu.

Um die andere Software vollständig zu deinstallieren, rufen Sie die Hersteller-Website auf und führen Sie das entsprechende Deinstallations-Tool aus oder wenden Sie sich direkt an den Hersteller, um eine Deinstallationsanleitung zu erhalten.

3. Starten Sie Ihr System im Normalmodus neu und installieren Sie Bitdefender erneut.

Sie haben die oben beschriebenen Schritte bereits durchgeführt und das Problem besteht weiterhin.

Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 76).
2. Nutzen Sie die Systemwiederherstellung von Windows, um den Computer zu einem früheren Zeitpunkt wiederherzustellen, bevor das Bitdefender-Produkt installiert wurde.
3. Starten Sie das System im Normalmodus neu und wenden Sie sich an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“* (S. 166) beschrieben.

24. MALWARE VON IHREM SYSTEM ENTFERNEN

Malware kann Ihr System auf vielfältige Art und Weise beeinflussen. Wie Bitdefender auf diese Malware reagiert, hängt von der Art des Malware-Angriffs ab. Da Viren ihr Verhalten ständig ändern, ist es schwierig ein Muster für ihr Verhalten und Aktionen festzulegen.

Es gibt Situationen, in denen Bitdefender eine Malware-Infizierung Ihres Systems nicht automatisch entfernen kann. In solch einem Fall ist Ihre Intervention nötig.

- *„Bitdefender-Rettungsmodus“* (S. 156)
- *„Wie gehe ich vor, wenn Bitdefender einen Virus auf Ihrem Computer findet?“* (S. 159)
- *„Wie entferne ich einen Virus aus einem Archiv?“* (S. 160)
- *„Wie entferne ich einen Virus aus einem E-Mail-Archiv?“* (S. 161)
- *„Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?“* (S. 163)
- *„Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?“* (S. 163)
- *„Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?“* (S. 164)
- *„Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?“* (S. 164)
- *„Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?“* (S. 164)

Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Bitdefender wie in Kapitel *„Hilfe anfordern“* (S. 166) beschrieben, kontaktieren.

24.1. Bitdefender-Rettungsmodus

Der **Rettungsmodus** ist eine Bitdefender-Funktion, mit der Sie alle bestehenden Festplattenpartitionen unabhängig von Ihrem Betriebssystem scannen und desinfizieren können.

Sobald Bitdefender Antivirus Plus 2016 installiert wurde, kann der Rettungsmodus genutzt werden, selbst wenn Sie Ihr System unter Windows nicht mehr hochfahren können.

Starten Ihres Systems im Rettungsmodus

Es gibt zwei Möglichkeiten, den Rettungsmodus zu starten:

Über die Bitdefender-Benutzeroberfläche

Um den Rettungsmodus direkt aus Bitdefender heraus zu starten, gehen Sie folgendermaßen vor:

1. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **Schutz**.
3. Wählen Sie im Modul **Virenschutz Rettungsmodus** aus.

   Ein Bestätigungsfenster wird angezeigt. Bitte klicken Sie auf **Ja**, um Ihren Computer neu zu starten.
4. Nach dem Neustart des Computers erscheint ein Menü, das Sie dazu auffordert, ein Betriebssystem auszuwählen. Wählen Sie **Bitdefender-Rettungsmodus** aus und drücken Sie die **Eingabetaste**, um den Computer in einer Bitdefender-Umgebung zu starten, in der Sie Ihre Windows-Partition bereinigen können.
5. Wenn Sie dazu aufgefordert werden, drücken Sie die **Enter**-Taste und wählen Sie die Bildschirmauflösung, die am ehesten der von Ihnen sonst verwendeten Auflösung entspricht. Drücken Sie die **Eingabetaste** erneut.

   Der Bitdefender-Rettungsmodus wird innerhalb weniger Momente geladen.

Starten des Computers im Rettungsmodus

Wenn Windows nicht mehr startet, können Sie Ihren Computer direkt im Bitdefender-Rettungsmodus neu starten, indem Sie folgendermaßen vorgehen:

1. Starten Sie Ihren Computer bzw. führen Sie einen Neustart durch und fangen Sie an, die **Leertaste** zu drücken, bevor das Windows-Logo erscheint.
2. Ein Menü erscheint und fordert Sie auf, ein Betriebssystem für den Start auszuwählen. Drücken Sie auf die **Tabulatortaste**, um in den Tools-Bereich zu wechseln. Wählen Sie **Bitdefender Rescue Image** und drücken Sie die **Eingabetaste**, um den Computer in einer

Bitdefender-Umgebung zu starten, von der aus Sie Ihre Windows-Partition bereinigen können.

3. Wenn Sie dazu aufgefordert werden, drücken Sie die **Enter**-Taste und wählen Sie die Bildschirmauflösung, die am ehesten der von Ihnen sonst verwendeten Auflösung entspricht. Drücken Sie die **Eingabetaste** erneut.

   Der Bitdefender-Rettungsmodus wird innerhalb weniger Momente geladen.

Scannen Ihres Systems im Rettungsmodus

Um Ihr System im Rettungsmodus zu scannen, gehen Sie folgendermaßen vor:

1. Starten Sie den Rettungsmodus, wie in Kapitel „Starten Ihres Systems im Rettungsmodus“ (S. 157) beschrieben.
2. Das Bitdefender-Logo wird angezeigt und der Kopiervorgang für die Virenschutz-Engines beginnt.
3. Ein Willkommensfenster wird angezeigt. Klicken Sie auf **Fortfahren**.
4. Ein Update der Virensignaturen wird gestartet.
5. Nach Abschluss des Updates wird das Fenster für den Bitdefender-Bedarf-Scan angezeigt.
6. Klicken Sie auf **Jetzt scannen**, wählen Sie in dem jetzt erscheinenden Fenster das Scan-Ziel aus und klicken Sie auf **Öffnen**, um den Scan zu starten.

   Wir empfehlen Ihnen, Ihre gesamte Windows-Partition zu scannen.

   ### Beachten Sie

   Wenn Sie den Rettungsmodus nutzen, werden Ihnen die Namen der Partitionen im Linux-Format angezeigt. Die Festplattenpartitionen werden angezeigt als sda1, was wahrscheinlich der Windows-Partition (C:) entspricht, sda2, was (D:) entspricht usw.

7. Warten Sie, bis der Scan abgeschlossen ist. Falls Malware gefunden wurde, folgen Sie den Anweisungen, um die Bedrohung zu entfernen.
8. Um den Rettungsmodus zu beenden, klicken Sie mit der rechten Maustaste auf einen leeren Bereich auf dem Desktop, klicken Sie im Kontextmenü

auf **Verlassen** und wählen Sie dann, ob Sie den Computer neu starten oder herunterfahren möchten.

24.2. Wie gehe ich vor, wenn Bitdefender einen Virus auf Ihrem Computer findet?

Es gibt verschiedene Möglichkeiten, Ihnen mitzuteilen, ob sich auf Ihrem Computer Viren befinden:

- Sie haben einen Scan durchgeführt und Bitdefender hat infizierte Einträge gefunden.
- Ein Virenwarnhinweis informiert Sie, dass Bitdefender einen oder mehrere Viren auf Ihrem Computer geblockt hat.

In solchen Situationen sollten Sie Bitdefender aktualisieren, um sicherzustellen, dass Sie über die neuesten Malware-Signaturen verfügen und einen System-Scan durchführen, um das System zu prüfen.

Sobald der System-Scan abgeschlossen ist, wählen Sie die gewünschte Aktion für die infizierten Objekte aus (Desinfizieren, Löschen, In Quarantäne verschieben).

Warnung
Wenn Sie den Verdacht haben, dass die Datei Teil des Windows-Betriebssystems ist oder dass es sich nicht um eine infizierte Datei handelt, folgen Sie NICHT diesen Schritten und kontaktieren Sie so bald wie möglich den Bitdefender-Kundendienst.

Falls die ausgewählte Aktion nicht durchgeführt werden konnte und im Scan-Protokoll ersichtlich ist, dass Ihr PC mit einer Bedrohung infiziert ist, die nicht gelöscht werden kann, müssen Sie die Datei(en) manuell entfernen.

Die erste Methode kann im Normalmodus eingesetzt werden:

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
   b. Wechseln Sie zum Reiter **Schutz**.
   c. Klicken Sie im Modul **Virenschutz** auf den Reiter **Schild**.
   d. Klicken Sie auf den Schalter, um **Zugriff-Scan** zu deaktivieren.

2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte „*Wie kann ich in Windows versteckte Objekte anzeigen?*“ (S. 74).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

Sollte die erste Methode, die Infizierung zu entfernen, fehlgeschlagen sein, gehen Sie folgendermaßen vor:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte „*Wie führe ich einen Neustart im abgesicherten Modus durch?*“ (S. 76).
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte „*Wie kann ich in Windows versteckte Objekte anzeigen?*“ (S. 74).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Starten Sie Ihren Computer neu und starten Sie den Normalmodus.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt „*Hilfe anfordern*“ (S. 166) beschrieben.

24.3. Wie entferne ich einen Virus aus einem Archiv?

Bei einem Archiv handelt es sich um eine Datei oder eine Dateisammlung, die mit einem speziellen Format komprimiert wurde, um so den benötigten Festplattenplatz zu reduzieren.

Einige dieser Formate sind offene Formate und bieten Bitdefender die Möglichkeit, diese zu scannen und die entsprechenden Aktionen durchzuführen, um sie zu entfernen.

Andere Archivformate sind teilweise oder komplett geschlossen und Bitdefender kann nur das Vorhandensein von Viren innerhalb dieser Archive feststellen, nicht jedoch andere Aktionen ausführen.

Wenn Bitdefender Sie darüber informiert, dass ein Virus innerhalb eines Archivs gefunden wurde und keine Aktion verfügbar ist, bedeutet dies, dass der Virus aufgrund möglicher Restriktionen der Zugriffseinstellungen des Archivs nicht entfernt werden kann.

So können Sie einen in einem Archiv gespeicherten Virus entfernen.

1. Führen Sie einen System-Scan durch, um das Archiv zu finden, in dem sich der Virus befindet.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
   b. Wechseln Sie zum Reiter **Schutz**.
   c. Klicken Sie im Modul **Virenschutz** auf den Reiter **Schild**.
   d. Klicken Sie auf den Schalter, um **Zugriff-Scan** zu deaktivieren.
3. Gehen Sie zum Speicherort des Archivs und dekomprimieren Sie es mit einem Archivierungsprogramm wie beispielsweise WinZip.
4. Identifizieren Sie die infizierte Datei und löschen Sie sie.
5. Löschen Sie das Originalarchiv, um sicherzugehen, dass die Infizierung vollständig entfernt ist.
6. Komprimieren Sie die Dateien erneut in einem neuen Verzeichnis und verwenden Sie dafür ein Komprimierprogramm wie WinZip.
7. Aktivieren Sie den Bitdefender-Echtzeit-Virenschutz und führen Sie einen Vollsystem-Scan durch, um so sicherzustellen, dass Ihr System nicht anderweitig infiziert ist.

Beachten Sie
Es ist wichtig zu beachten, dass ein in einem Archiv gespeicherter Virus für Ihr System keine unmittelbare Bedrohung darstellt, da der Virus dekomprimiert und ausgeführt werden muss, bevor er Ihr System infizieren kann.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 166)* beschrieben.

24.4. Wie entferne ich einen Virus aus einem E-Mail-Archiv?

Bitdefender kann auch Viren in E-Mail-Datenbanken und in auf Festplatten gespeicherten E-Mail-Archiven aufspüren.

Manchmal ist es notwendig, die infizierte Nachricht über die im Scan-Bericht zur Verfügung gestellten Informationen zu identifizieren und sie dann manuell zu löschen.

So können Sie in einem E-Mail-Archiv gespeicherte Viren entfernen:

1. Scannen Sie die E-Mail-Datenbank mit Bitdefender.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie unten links in der Bitdefender-Benutzeroberfläche auf das -Symbol.
   b. Wechseln Sie zum Reiter **Schutz**.
   c. Klicken Sie im Modul **Virenschutz** auf den Reiter **Schild**.
   d. Klicken Sie auf den Schalter, um **Zugriff-Scan** zu deaktivieren.
3. Öffnen Sie den Scan-Bericht und nutzen Sie die Identifikationsinformation (Betreff, Von, An) der infizierten Nachricht, um den dazugehörigen E-Mail-Client zu finden.
4. Löschen Sie die infizierte Nachricht. Die meisten E-Mail-Clients verschieben gelöschte Nachrichten in ein Wiederherstellungsordner, von dem aus sie wiederhergestellt werden können. Sie sollten sicherstellen, dass die Nachricht auch aus diesem Recovery-Verzeichnis gelöscht ist.
5. Komprimieren Sie das Verzeichnis, in dem die infizierte Nachricht gespeichert wird.
   - In Outlook Express: Klicken Sie im Dateimenü auf "Verzeichnis", dann auf "Alle Verzeichnisse komprimieren".
   - In Microsoft Outlook 2007: Klicken Sie im Dateimenü auf "Datendateiverwaltung". Wählen Sie das persönliche Verzeichnis (.pst), das Sie komprimieren möchten und klicken Sie auf "Einstellungen". Klicken Sie auf Jetzt komprimieren.
   - In Microsoft Outlook 2010 / 2013: Klicken Sie im Dateimenü auf Info und dann Kontoeinstellungen (Konten hinzufügen oder entfernen bzw. vorhandene Verbindungseinstellungen ändern). Klicken Sie danach auf Datendatei, markieren Sie die persönlichen Ordner-Dateien (.pst), die Sie komprimieren wollen, und klicken Sie auf Einstellungen. Klicken Sie auf Jetzt komprimieren.
6. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 166)* beschrieben.

24.5. Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?

Möglicherweise halten Sie eine Datei auf Ihrem System für gefährlich, obwohl Ihr Bitdefender-Produkt keine Gefahr erkannt hat.

Um sicherzustellen, dass Ihr System geschützt ist, gehen Sie folgendermaßen vor:

1. Führen Sie einen **System-Scan** mit Bitdefender durch. Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie scanne ich mein System?“ (S. 62)*.
2. Wenn der Scan ein sauberes Ergebnis liefert, Sie aber weiterhin Zweifel an der Sicherheit der Datei hegen und ganz sicher gehen möchten, wenden Sie sich bitte an unsere Support-Mitarbeiter, damit wir Ihnen helfen können.

   Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Hilfe anfordern“ (S. 166)*.

24.6. Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?

Dies ist nur eine Benachrichtigung, dass die von Bitdefender gefundenen Dateien entweder passwortgeschützt oder anderweitig verschlüsselt sind.

Am häufigsten sind passwortgeschützte Objekte:

- Dateien, die zu einer anderen Sicherheitslösung gehören.
- Dateien, die zum Betriebssystem gehören.

Um die Inhalte tatsächlich zu scannen, müssen diese Dateien entweder extrahiert oder anderweitig entschlüsselt werden.

Sollten diese Inhalte extrahiert werden, wird der Echtzeit-Scanner von Bitdefender diese automatisch scannen, um so den Schutz Ihres Computers zu gewährleisten. Wenn Sie diese Dateien mit Bitdefender scannen möchten, müssen Sie den Produkthersteller kontaktieren, um nähere Details zu diesen Dateien zu erhalten.

Unsere Empfehlung ist, diese Dateien zu ignorieren, da Sie für Ihr System keine Bedrohung darstellen.

24.7. Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?

Alle Dateien, die im Scan-Protokoll als "Übersprungen" ausgewiesen werden, sind sauber.

Für eine bessere Leistung scannt Bitdefender keine Dateien, die seit dem letzten Scan nicht verändert wurden.

24.8. Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?

Die zu stark komprimierten Objekte sind Elemente, die durch die Scan-Engine nicht extrahiert werden konnten oder Elemente, für die eine Entschlüsselung zu viel Zeit in Anspruch genommen hätte und die dadurch das System instabil machen würden.

Überkomprimiert bedeutet, dass Bitdefender das Scannen von Archiven übersprungen hat, da das Entpacken dieser zu viele Systemressourcen in Anspruch genommen hätte. Der Inhalt wird, wenn nötig, in Echtzeit gescannt.

24.9. Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?

Wird eine infizierte Datei gefunden, versucht Bitdefender automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

Dies geschieht normalerweise bei Installationsdateien, die von nicht vertrauenswürdigen Seiten heruntergeladen werden. Wenn Sie auf ein solches Problem stoßen, laden Sie die Installationsdatei von der Website des Herstellers oder einer anderen vertrauenswürdigen Website herunter.

KONTAKTIEREN SIE UNS

25. HILFE ANFORDERN

Bitdefender bietet seinen Kunden konkurrenzlos schnellen und kompetenten Support. Sollten sich Probleme ergeben oder Sie eine Frage zu Ihrem Bitdefender-Produkt haben, so stehen Ihnen verschiedene Online-Quellen zur Verfügung, wo Sie Lösungen und Antworten finden. Sie können sich auch jederzeit an den Bitdefender-Kundendienst wenden. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

Im Abschnitt *„Verbreitete Probleme beheben“* (S. 141) finden Sie alle wichtigen Informationen zu den häufigsten Problemen, die bei der Verwendung dieses Produkts auftreten können.

Wenn Sie in den vorhandenen Quellen keine Antwort auf Ihre Frage finden, können Sie uns direkt kontaktieren:

- „Kontaktieren Sie uns direkt aus Ihrem Bitdefender-Produkt heraus“ (S. 166)
- „Kontaktieren Sie uns über unser Online-Support-Center“ (S. 167)

Kontaktieren Sie uns direkt aus Ihrem Bitdefender-Produkt heraus

Wenn Sie über eine aktive Internet-Verbindung verfügen, können Sie Bitdefender direkt aus der Benutzeroberfläche heraus kontaktieren, um Hilfe zu erhalten.

Folgen Sie diesen Schritten:

1. Klicken Sie oben in der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie den Punkt **Hilfe & Support** aus dem Menü aus.
2. Sie haben die folgenden Möglichkeiten:
   - **Produktdokumentation**

     Hier können Sie unsere Datenbank nach den gewünschten Informationen durchsuchen.
   - **Support kontaktieren**

     Sie können über die Schaltfläche **Kundendienst kontaktieren** das Bitdefender-Support-Tool aufrufen und den Kundendienst kontaktieren.

Über die Schaltfläche **Weiter** können Sie im Assistenten blättern. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

a. Markieren Sie das Zustimmungskästchen und klicken Sie auf **Weiter**.

b. Geben Sie in das Formular die nötigen Daten ein:

   i. Geben Sie Ihre E-Mail-Adresse ein.

   ii. Geben Sie Ihren vollen Namen ein.

   iii. Beschreiben Sie im Textfeld das Problem, das aufgetreten ist.

   iv. Nutzen Sie die Option **Versuchen Sie, das Problem vor der Übertragung zu reproduzieren**, falls Probleme mit dem Produkt auftreten. Fahren Sie mit den erforderlichen Schritten fort.

c. Bitte warten Sie einige Minuten, während Bitdefender die produkt-relevanten Informationen einholt. Diese Informationen helfen unseren Mitarbeitern, eine Lösung für Ihr Problem zu finden.

d. Klicken Sie auf **Beenden**, um die Information an den Bitdefender-Kundendienst zu senden. Sie werden möglichst bald kontaktiert.

Kontaktieren Sie uns über unser Online-Support-Center

Wenn Sie über das Bitdefender-Produkt nicht auf die notwendigen Informationen zugreifen können, wenden Sie sich bitte an unser Online-Support-Center.

1. Gehen Sie zu http://www.bitdefender.de/support/consumer.html.

   Im Bitdefender-Support-Center finden Sie eine Vielzahl von Beiträgen, die Lösungen zu Problemen im Zusammenhang mit Bitdefender bereithalten.

2. Nutzen Sie die Suchleiste oben im Fenster, um Artikel zu finden, die eine Lösung für Ihr Problem enthalten könnten. Geben Sie dazu einen Begriff in die Suchleiste ein und klicken Sie auf **Suchen**.

3. Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.

4. Wenn die dort vorgeschlagene Lösung das Problem nicht behebt, gehen Sie zu

http://www.bitdefender.de/support/contact-us.htmlund kontaktieren Sie unseren Kundendienst.

26. ONLINE-RESSOURCEN

Für die Lösung Ihres Problems und Fragen im Zusammenhang mit Bitdefender stehen Ihnen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:

  http://www.bitdefender.de/support/consumer.html

- Bitdefender Support-Forum:

  http://forum.bitdefender.com

- Das Computer-Sicherheitsportal HOTforSecurity:

  http://www.hotforsecurity.com

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

26.1. Bitdefender-Support-Center

Das Bitdefender-Support-Center ist eine Online-Sammlung von Informationen zu Ihren Bitdefender-Produkten. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Virenvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Das Bitdefender-Support-Center ist öffentlich zugänglich und frei durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. Alle berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Support-Center wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Das Bitdefender-Support-Center steht Ihnen jederzeit unter der folgenden Adresse zur Verfügung:

http://www.bitdefender.de/support/consumer.html.

26.2. Bitdefender Support-Forum

Das Bitdefender Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, Hilfe zu erhalten oder anderen Hilfestellung zu geben.

Falls Ihr Bitdefender-Produkt nicht richtig funktioniert, bestimmte Viren nicht von Ihrem Computer entfernen kann oder wenn Sie Fragen über die Funktionsweise haben, stellen Sie Ihr Problem oder Frage in das Forum ein.

Support-Techniker von Bitdefender überwachen neue Einträge in das Forum, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie bitte im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter http://forum.bitdefender.com. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Für den Zugriff auf den Bereich Konsumgüter klicken Sie bitte auf **Schutz für Privatanwender**.

26.3. Das Portal HOTforSecurity

HOTforSecurity bietet umfangreiche Informationen rund um das Thema Computer-Sicherheit. Hier erfahren Sie mehr über die verschiedenen Bedrohungen, denen Ihr Computer während einer bestehenden Internetverbindung ausgesetzt ist (Malware, Phishing, Spams, Cyber-Kriminelle).

Ständig werden neue Artikel zu den neuesten Threats, aktuellen Sicherheitstrends und anderen Informationen zur Computersicherheits-Branche eingestellt, damit Sie up-to-date bleiben.

Die Adresse von HOTforSecurity ist http://www.hotforsecurity.com.

27. KONTAKTINFORMATION

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. Seit mehr als 10 Jahren überbietet BITDEFENDER konstant die bereits hochgesteckten Erwartungen seiner Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

27.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Support-Center:http://www.bitdefender.de/support/consumer.html
Dokumentation: documentation@bitdefender.com
Händler vor Ort:http://www.bitdefender.de/partners
Partnerprogramm: partners@bitdefender.com
Medienkontakt: pr@bitdefender.com
Karriere: jobs@bitdefender.com
Viruseinsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Missbrauch melden: abuse@bitdefender.com
Website:http://www.bitdefender.de

27.2. Lokale Vertriebspartner

Bitdefender-Händler stehen für vertriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung.

So finden Sie einen Bitdefender-Händler in Ihrem Land:

1. Gehen Sie zu http://www.bitdefender.com/partners/partner-locator.html.
2. Geben Sie über die entsprechenden Optionen Ihren Wohnort und Ihr Land an.
3. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren. Bitte schreiben Sie uns Ihre Email in englischer Sprache, damit wir Ihnen umgehend helfen können.

27.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur

Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefon (Geschäftsstelle&Vertrieb): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Technischer Support: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.com

Deutschland

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Geschäftsstelle: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vertrieb: vertrieb@bitdefender.de
Technischer Support: http://www.bitdefender.de/support/consumer.html
Web: http://www.bitdefender.de

Spain

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Vertrieb: comercial@bitdefender.es
Technischer Support: http://www.bitdefender.es/support/consumer.html
Website: http://www.bitdefender.es

Rumänien

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest

Fax: +40 21 2641799
Telefon Vertrieb: +40 21 2063470
Vertrieb E-Mail: sales@bitdefender.ro
Technischer Support: http://www.bitdefender.ro/support/consumer.html
Website: http://www.bitdefender.ro

Vereinigte Arabische Emirate

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefon Vertrieb: 00971-4-4588935 / 00971-4-4589186
Vertrieb E-Mail: mena-sales@bitdefender.com
Technischer Support: http://www.bitdefender.com/support/consumer.html
Website: http://www.bitdefender.com

Glossar

Abonnement

Ein Kaufvertrag, der Benutzern das Recht einräumt, ein bestimmtes Produkt oder eine Dienstleistung auf einer bestimmten Anzahl von Geräten und für einen bestimmten Zeitraum in Anspruch zu nehmen. Ein abgelaufenes Abonnement kann unter Verwendung der vom Nutzer beim Ersterwerb angegebenen Informationen automatisch verlängert werden.

Advanced Persitent Threats

Advanced Persistent Threat (APT) nutzen Sicherheitslücken im System, um wichtige Daten zu stehlen und an ihre Quellen zu übermitteln. Organisationen, Unternehmen und Regierungsbehörden sind eine große Zielgruppe, die von dieser Malware-Gattung ins Visier genommen wird.

Advanced Persistent Threats sollen so lange wie möglich unentdeckt bleiben. Während dieser Zeit sollen sie das System überwachen und wichtige Daten sammeln, ohne dabei die Zielcomputer zu beschädigen. Eingebracht wird der Virus in das Netzwerk durch PDF-Dateien oder Office-Dokumente, die keinen Verdacht erregen, so dass jeder Benutzer diese Dateien ausführen kann.

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

AktiveX

ActiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die ActiveX Technologie wird von Microsofts Internet Explorer benutzt,

damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit ActiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. ActiveX-Steuerelemente werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

Aktivierungs-Code

Dabei handelt es sich um einen eindeutigen Schlüssel, der käuflich erworben und zur Aktivierung eines Produkts oder eines Dienstes verwendet werden kann. Mit einem Aktivierungscode kann ein gültiges Abonnement für einen bestimmten Zeitraum und eine bestimmte Anzahl an Geräten aktiviert werden. Zudem kann mit einem solchen Code eine Abonnement verlängert werden, solange es sich auf das gleiche Produkt oder den gleichen Dienst bezieht.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten

Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Boot-Sektor:
Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus
Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie
In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Dateierweiterung
Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Download

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

Durchsuchen

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Bekannte Browser sind Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Dies sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

E-Mail

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

E-Mail Client

Ein E-Mail Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Scan-Methode benötigt keine spezifischen Virussignaturen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante eines alten Virus getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java Applet

Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) an, die das Applet einnehmen kann. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets z. B. auf dem Client laufen, können diese keine Daten auf der Maschine des Clients lesen oder schreiben. Zusätzlich sind die Applets dahingehend beschränkt, dass sie nur Daten aus der Domain lesen und schreiben können, zu der sie gehören.

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Komprimierte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, mit denen Dateien komprimiert werden können, sodass diese weniger Speicherplatz benötigen. Zum Beispiel: Angenommen, Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise belegen diese Leerzeichen dann 10 Bytes an Speicherplatz.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein Sonderzeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden. In diesem Fall sind nur noch zwei Bytes notwendig statt zehn. Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den geprüften Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Nicht heuristisch

Diese Scan-Methode beruht auf spezifischen Virussignaturen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einem Scheinvirus getäuscht werden kann und so Fehlalarme verhindert.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Beim Phishing wird eine E-Mail mit betrügerischer Absicht an einen Empfänger gesendet, wobei vorgetäuscht wird, die E-Mail stamme von einem bekannten und seriösen Unternehmen. Zweck dieser E-Mail ist es dann, vertrauliche Benutzerdaten wie Passwörter und/oder Kreditkartennummern zu erhalten. Die E-Mail führt den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Photon

Photon ist eine innovative und unaufdringliche Bitdefender-Technologie, die eigens entwickelt wurde, um die Auswirkungen des Virenschutzes auf die Systemleistung zu minimieren. Durch die Hintergrundüberwachung aller PC-Aktivitäten werden Nutzungsprofile erstellt, mit denen Start- und Scan-Prozesse optimiert werden können.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Ransomware

Bei Ransomware handelt es sich um schädliche Programme, die anfällige Systeme für den Benutzer sperren und für deren Freigabe Lösegeld erpressen. CryptoLocker, CryptoWall und TeslaWall sind nur einige Beispiele für Ransomware, die es auf Benutzercomputer abgesehen haben.

Die Infektion kann sich durch das Aufrufen eine Spam-Nachricht, das Herunterladen eines E-Mail-Anhangs oder die Installation von Anwendungen ausbreiten, ohne dass der Benutzer es überhaupt bemerkt. Ransomware-Hacker nehmen herkömmliche Benutzer und Unternehmen ins Visier.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet

und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Speicherauslastung

Interne Speicherbereiche im Rechner. Der Begriff Arbeitsspeicher bezeichnet Datenträger in Form von sehr schnellen Chips. Dies steht im Gegensatz zu Speicherplatz, der sich auf Magnetbändern oder

Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher. Dieser wird auch Hauptspeicher oder RAM bezeichnet.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

Jede Datei, die sich in diesem Ordner befindet, wird geöffnet, wenn der Rechner gestartet wird. Das können z. B. ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder auch Anwendungen sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information

und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können ebenso schädlich sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update-Server

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über ein eigenes Update-Modul, das manuelle oderautomatische Scans nach Updates ermöglicht.

Virus

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will

oder merkt. Die meisten Viren können sich auch selbst vervielfältigen. Alle Computerviren wurden von Menschen programmiert. Ein Virus, der sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

Virussignatur

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.